4 Реферати

УДК 354:007

ВІДПОВІДАЛЬНІСТЬ ЗА ПОРУШЕННЯ ВИМОГ ЗАКОНОДАВСТВА В СФЕРІ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

Олексій Мервінський
Державна служба України з питань захисту персональних даних

Стаття: ***6 стор., 5 джерел.***

Питання відповідальності за порушення законодавства про захист персональних даних насамперед слід тлумачити з огляду на дії або бездіяльність, що спричинили реальну суттєву шкоду фізичній особі внаслідок незаконного доступу до її персональних даних та незаконної обробки цих даних. Найбільш важливою нормою щодо відповідальності за порушення законодавства про захист персональних даних слід вважати статтю 182 Кримінального кодексу України "Порушення недоторканності приватного життя», яка передбачає відповідальність за: незаконне збирання, зберігання, використання, знищення, поширення конфіденційної інформації про особу або незаконну зміну такої інформації. Далі за «ступенем захисту від втручання в особисте життя» слідують статті 188[39] (порушення законодавства у сфері захисту персональних даних) та 188[40] (невиконання законних вимог посадових осіб спеціально уповноваженого центрального органу виконавчої влади з питань захисту персональних даних) Кодексу України про адміністративні правопорушення. Особлива важливість зазначених статей пов’язана з тим, що вони покликані унеможливити зловживання та незаконне використання персональних даних, що могло б завдати шкоди суб’єкту персональних даних - людині.

І тільки як крайній захід в законодавстві передбачається відповідальність з ухилення від державної реєстрації бази персональних даних та неповідомлення або несвоєчасне повідомлення спеціально уповноваженого центрального органу виконавчої влади з питань захисту персональних даних про зміну відомостей, що подаються для державної реєстрації бази персональних даних. Це пов’язано з тим, що ухилення від реєстрації само по собі, зазвичай, не завдає шкоди суб’єкту персональних даних, але створює передумови для інших порушень.

До основних факторів, що визначають умови настання відповідальності володільців або розпорядників баз персональних даних, доцільно віднести їх дії, які пов’язані з:

- персональними даними без згоди суб’єкта персональних даних;
- порушенням вимог щодо забезпечення законності обробки персональних даних;
- невиконанням або неналежним виконанням процедур, пов’язаних з формулюванням мети обробки персональних даних;
- недотриманням вимог щодо точності та достовірності персональних даних, які збираються та обробляються у базах персональних даних;
- порушенням формування складу та змісту персональних даних у базі персональних даних;
- невиконанням вимог, пов’язаних з державною реєстрацією бази персональних даних;
- порушенням порядку обробки персональних даних;
- ненаданням або несвоєчасним наданням суб’єкту персональних даних доступу до його персональних даних, що містяться у відповідній базі персональних даних;
- відсутністю умов для захисту персональних даних у базі персональних даних;
- порушенням вимог при поширенні (розповсюдженні, реалізації, передачі) відомостей про фізичну особу з урахуванням того, що виконання вимог встановленого режиму захисту персональних даних забезпечує сторона, що поширює ці дані.

ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ ТРЕБОВАНИЙ ЗАКОНОДАТЕЛЬСТВА В СФЕРЕ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Алексей Мервинский
Государственная служба Украины по вопросам защиты персональных

Вопрос ответственности за нарушение законодательства о защите персональных данных в первую очередь следует объяснять учитывая действия или бездеятельность, которые повлекли реальный существенный вред физическому лицу в результате незаконного доступа к его персональным данным и незаконной обработке этих данных.

Наиболее важной нормой относительно ответственности за нарушение законодательства о защите персональных данных следует считать статью 182 Криминального кодекса Украины "Нарушения неприкосновенности частной жизни», которая предусматривает ответственность за незаконный сбор, хранение, использование, уничтожение, распространение конфиденциальной информации о лице или незаконном изменении такой информации.

Дальше за «степенью защиты от вмешательства в личную жизнь» следуют статьи 188^{39} (нарушение законодательства в сфере защиты персональных данных) и 188^{40} (невыполнение законных требований должностных лиц специально уполномоченного центрального органа исполнительной власти по вопросам защиты персональных данных) Кодекса Украины об административных правонарушениях. Особенная важность отмеченных статей связана с тем, что они призваны сделать невозможным злоупотребление и незаконное использование персональных данных, которые могли бы навредить субъекту персональних даннях – человеку. И только как крайняя мера в законодательстве предусматривается ответственность за уклонения от государственной регистрации базы персональных данных и несообщения или несвоевременное сообщение специально уполномоченного центрального органа исполнительной власти по вопросам защиты персональных данных об изменении сведений, которые подаются для государственной регистрации базы персональных данных.

Это связано с тем, что уклонение от регистрации само по себе, обычно, не наносит вред субъекту персональных данных, но создает предпосылки для других нарушений.

К основным факторам, которые определяют условия наступления ответственности владельцев или распорядителей баз персональных данных, целесообразно отнести их действия, которые связаны с:

- персональными данными без согласия субъекта персональных данных;
- нарушением требований относительно обеспечения законности обработки персональных данных; - невыполнением или неподобающим выполнением процедур, связанных с формулировкой цели обработки персональных данных;
- несоблюдением требований относительно точности и достоверности персональных данных, которые собираются и обрабатываются в базах персональных данных;
- нарушением формирования состава и содержания персональных данных в базе персональных данных;
- невыполнением требований, связанных с государственной регистрацией базы персональных данных;
- нарушением порядка обработки персональных данных;
- непредоставлением или несвоевременным предоставлением субъекту персональных данных доступа к его персональным данным, которые содержатся в соответствующей базе персональных данных;
- отсутствием условий для защиты персональных данных в базе персональных данных;
- нарушением требований при распространении, реализации, передаче сведений о физическом лице с учетом того, что выполнение требований установленного режима защиты персональных данных обеспечивает сторона, которая распространяет эти данные.

RESPONSIBILITY FOR VIOLATION OF REQUIREMENTS OF LEGISLATION IN THE SPHERE OF PROTECTION OF THE PERSONAL DATA

Oleksij Mervinskiy
State service of Ukraine on personal data protection

The question of responsibility for violation of legislation about the protection of the personal data above all things it should be given to explain taking into account actions or inactivity, that entailed the real substantial harm a physical person as a result of illegal access to its personal information and illegal processing of these data. By the most essential norm in relation to responsibility for violation of legislation about the protection of the personal data it follows to count the article 182 of the Criminal Code of Ukraine (3) about "Violation of inviolability of private life», which foresees responsibility after: illegal collection, storage, use, elimination, distribution of confidential information, is about a person or illegal change of such information.

Farther after the «degree of protecting from interference with the personal life» follow the article 188^{39} (violation of legislation is in the field of protection of the personal data) and 188^{40} (non-fulfillment of legal requirements of public servants of the specially authorized central organ of executive power is on questions the protection of the personal data) Code of Ukraine about administrative offences. The special importance of the noted articles is related to that they are called to do impossible abuse and illegal use of the personal information, which would inflict harm the subject of the personal information - man.

And only as an extreme measure in a legislation is foreseen responsibility from avoiding state registration of base of the personal information and non-disclosure or ill-timed report of the specially authorized central organ of executive power on questions the protection of the personal data about the change of information which are given for state registration of base of the personal information.

To the basic factors which determine the terms of offensive of responsibility of proprietors or managers of bases of the personal information, it is expedient to take their actions which are CPLD from:

- by the personal information without the consent of subject of the personal information;
- by violation of requirements in relation to providing of legality of processing of the personal data;
- by non-fulfillment or improper implementation of procedures, related to formulation of purpose of processing of the personal data;
- by a failure to observe of requirements in relation to exactness and authenticity of the personal information which going and processed in the bases of the personal information;
- by violation of forming of composition and maintenance of the personal information in the base of the personal information;
- by non-fulfillment of requirements, related to state registration of base of the personal information;
- disturbing processing of the personal data;- by an ungrant or ill-timed grant the subject of the personal information of access to his personal information which are contained in the proper base of the personal information;
- by absence of terms for the protection of the personal data in the base of the personal information;
- by violation of requirements at distribution (distribution, realization, transmission) of information about a physical person taking to account that implementation of requirements of the set mode of protection of the personal data is provided by a side which diffuses these information.

УДК 654.924

ОСОБЛИВОСТІ ОЦІНКИ ТРИВАЛОСТІ НЕСАНКЦІОНОВАНОГО ПРОНИКНЕННЯ НА ОБ'ЄКТ, ЩО ОХОРОНЯЄТЬСЯ

Володимир Волхонський

Санкт-петербурзький національний дослідницький університет інформаційних технологій, механіки і оптики

Стаття: ***6 стор., 4 джерел.***

Для оцінки ефективності систем безпеки (СБ) необхідна оцінка тривалості несанкціонованого проникнення (НП) для порівняння з часом реакції СБ на НП. Як характерні точки маршруту проникнення можуть бути вибрані зони об'єкту і перешкоди. Переміщення між такими точками можна трактувати як переходи від початку i-ї зони до початку j-ї зони; від початку i-ї зони до початку j-ї перешкоди; подолання i-ї перешкоди з переходом в j-у зону з тривалістю T_{ij}. Сукупність всіх можливих переходів c_{ij} складає множину $\mathbf{C}$ переходів, яку можна представити матрицею $\mathbf{C}_{IJ}$ з елементами $c_{ij} = 0, \quad c_{ij} \notin \mathbf{C}$ або $c_{ij} = 1, \quad c_{ij} \in \mathbf{C}$. При необхідності обліку більш «тонких» особливостей переходів елементи матриці можуть визначати, наприклад, вірогідність вибору переходів або вірогідність їх виявлення. Певна

послідовність переходів $R_n = \{c_{ij}, c_{jk}, ..., c_{nm}, c_{ml}\}$ являє собою n-й маршрут НП. Загальна тривалість T_{Rn} проходження маршруту визначатиметься сумою тривалості окремих переходів. Переходи і маршрути можуть бути безальтернативними і альтернативними; що виявляються і не виявляються; незалежними $\mathbf{C}_m \bigcap \mathbf{C}_n = \varnothing$ і залежними $\mathbf{C}_m \bigcap \mathbf{C}_n \neq \varnothing$. Тривалість T_{ij} є випадковою величиною. Точнішу оцінку тривалості переходу при заданій вірогідності $p(t_{ij})$ його реалізації дає облік виду кривої щільності розподілу вірогідності $p(t_{ij})$ тривалості переходу. У припущенні близького вкладу складових в загальну суму $T_{Rn} = \sum_{Rn} T_{ij}$ можна говорити про нормалізацію щільності розподілу вірогідності загального часу проникнення. Оцінка $\hat{P}_{Rn}$ вірогідності того, що тривалість проходження всього маршруту буде не менш заданого значення T_{Rn}^{min} визначатиметься як $\hat{P}_{Rn} = \int_{T_{Rn}^{\min}}^{\infty} p(t_{Rn}) dt_{Rn}$. Задана вірогідність припинення проникнення визначить оцінку $\hat{T}_3^{max}$ максимально допустимої затримки прибуття групи реагування. При використання правила «3-х сігма» бажано прагнути до виконання умови $m_{Rn} >> 3\sigma_{Rn}$ Це дозволяє визначити оцінку вірогідності досягнення значення T_{Rn}^{min}, інтегруючи в межах від $m_{Rn} - 3\sigma_{Rn}$ до ∞.

ОСОБЕННОСТИ ОЦЕНКИ ПРОДОЛЖИТЕЛЬНОСТИ НЕСАНКЦИОНИРОВАННОГО ПРОНИКНОВЕНИЯ НА ОХРАНЯЕМЫЙ ОБЪЕКТ

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

Для оценки эффективности систем безопасности (СБ) необходима оценка продолжительности несанкционированного проникновения (НП) для сравнения со временем реакции СБ на НП. В качестве характерных точек маршрута проникновения могут быть выбраны зоны объекта и препятствия. Перемещения между такими точками можно трактовать как переходы от начала i-й зоны до начала j-й зоны; от начала i-й зоны до начала j-о препятствия; преодоления i-о препятствия с переходом в j-ю зону с продолжительностью T_{ij}. Совокупность всех возможных переходов c_{ij} составляет множество $\mathbf{C}$ переходов, которое можно представить матрицей $\mathbf{C}_{IJ}$ с элементами $c_{ij} = 0, \quad c_{ij} \notin \mathbf{C}$ или $c_{ij} = 1, \quad c_{ij} \in \mathbf{C}$. При необходимости учета более «тонких» особенностей переходов элементы матрицы могут определять, например, вероятности выбора переходов или вероятности их обнаружения. Определенная последовательность переходов $R_n = \{c_{ij}, c_{jk}, ..., c_{nm}, c_{ml}\}$ представляет собой n-й маршрут НП. Общая продолжительность T_{Rn} прохождения маршрута будет определяться суммой продолжительностей отдельных переходов. Переходы и маршруты могут быть безальтернативными и альтернативными; обнаруживаемыми и не обнаруживаемыми; независимыми $\mathbf{C}_m \bigcap \mathbf{C}_n = \varnothing$ и зависимыми $\mathbf{C}_m \bigcap \mathbf{C}_n \neq \varnothing$. Продолжительности T_{ij} представляют собой случайные величины. Более точную оценку продолжительности перехода при заданной вероятности его реализации дает учет вида кривой плотности распределения вероятности $p(t_{ij})$ продолжительности перехода. В предположении близкого вклада составляющих в общую сумму $T_{Rn} = \sum_{Rn} T_{ij}$ можно говорить о нормализации плотности распределения вероятности общего времени проникновения. Оценка $\hat{P}_{Rn}$ вероятности того, что продолжительность прохождения всего маршрута будет

не менее заданного значения T_{Rn}^{min} будет определяться как $\hat{P}_{Rn} = \int_{T_{Rn}^{\min}}^{\infty} p(t_{Rn})dt_{Rn}$. Заданная вероятность пресечения проникновения определит оценку $\hat{T}_3^{max}$ максимально допустимой задержки прибытия группы реагирования. При использования правила «3-х сигма» желательно стремиться к выполнению $m_{Rn} >> 3\sigma_{Rn}$. Что позволяет определить оценку вероятности достижения значения T_{Rn}^{min}, интегрируя в пределах от $m_{Rn} - 3\sigma_{Rn}$ до ∞.

THE SPECIAL FEATURES OF ESTIMATION OF DURATION INTRUSION ON PROTECTED OBJECT

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

Estimation of intrusion duration is necessary in order to estimate security system (SS) effectiveness based on comparison with SS reaction. During intrusion such specific points of route as object zones and physical obstacles could be chosen. Moving between such points may be interpreted as crossing from beginning of i zone to beginning of j zone; from beginning of i zone to beginning of j physical obstacles; overcoming of i physical obstacles to j zone with T_{ij} duration. All possible c_{ij} crossing are $\mathbf{C}$ set of crossing, which could be represented as $\mathbf{C}_{IJ}$ matrix with elements either $c_{ij} = 0, \quad c_{ij} \notin \mathbf{C}$ or $c_{ij} = 1, \quad c_{ij} \in \mathbf{C}$. More detailed description can include probability of crossing choice or their detection, for example. Certain chain of crossing $R_n = \{c_{ij}, c_{jk}, ..., c_{nm}, c_{ml}\}$ is n route of intrusion. Total duration T_{Rn} of route is sum of crossing duration. Routes and crossing could be alternative and non- alternative; detectable or non- detectable; undependable $\mathbf{C}_m \bigcap \mathbf{C}_n = \varnothing$ or dependable $\mathbf{C}_m \bigcap \mathbf{C}_n \neq \varnothing$. T_{ij} duration is random value. More exact estimation of crossing duration at certain probability of its choice could be based on certain type of $p(t_{ij})$ curve of distribution probability density of crossing duration. Assuming that each crossing creates similar contribution to total sum $T_{Rn} = \sum_{Rn} T_{ij}$ possible to speak about normalization of total intrusion duration. Estimation of $\hat{P}_{Rn}$ probability that total route duration will be not less then required T_{Rn}^{min} could be get as $\hat{P}_{Rn} = \int_{T_{Rn}^{\min}}^{\infty} p(t_{Rn})dt_{Rn}$. Requirement to probability of intrusion elimination will determine $\hat{T}_{\text{Ç}}^{max}$ estimation of maximum acceptable delay in reaction. Base on "3-sigma" rule $m_{Rn} >> 3\sigma_{Rn}$ ratio could be used for integration limits choice from $m_{Rn} - 3\sigma_{Rn}$ to ∞ in order to calculate estimation of probability of T_{Rn}^{min} realization.

УДК 347.83(477)

ПРАВОВІ ЗАСАДИ ІНФОРМАЦІЙНИХ ВІДНОСИН В УКРАЇНІ – НОВІ РЕАЛІЇ

Дарія Прокоф'єва-Янчиленко
Служба безпеки України

Стаття: ***11 стор., 21 джерел.***

З 01 січня 2011 року набув чинності Закон України «Про захист персональних даних», спрямований на впровадження всеохоплюючого механізму захисту персональних даних, які збираються, обробляються та/або зберігаються будь-якою фізичною чи юридичною особою на території України. Також з 09 травня набрали чинності Закон України «Про доступ до публічної інформації» та нова редакція Закону України «Про інформацію», ухвалені парламентом 13 січня 2011 року. Зазначені нормативно-правові акти істотно змінили існуюче правове поле інформаційної діяльності в Україні, тому заслуговують на увагу наукової спільноти, юристів-практиків та широких кіл громадськості.

За результатами проведеного огляду слід дійти висновку, що наявний пакет «інформаційних законів» навряд чи можуть вважатися гідною заміною попередньої редакції Закону України «Про інформацію», яка носила комплексний характер. Продовжують існувати численні колізії між правом на інформацію, правом доступу до інформації та необхідністю забезпечувати недоторканість приватного життя, принципами інформаційної глобалізації та необхідністю забезпечення безпеки інформаційного простору. Такий стан речей буде зберігатися ще досить довго і може бути виправлений лише тоді, коли наріжним каменем для розробки інформаційного законодавства стане саме інформація (як об'єкт правовідносин та цивілізаційний феномен в умовах реалізації концепції сталого розвитку), її система та структура (в т.ч. чітке розмежування на види та категорії за режимом доступу), а також відповідні права учасників відносин, що складаються з приводу інформації, та інформаційна безпека.

ПРАВОВЫЕ ПРИНЦИПЫ ИНФОРМАЦИОННЫХ ОТНОШЕНИЙ В УКРАИНЕ – НОВЫЕ РЕАЛИИ

Дария Прокофьева-Янчиленко
Служба безопасности Украины

С 01 января 2011 года вступил в силу Закон Украины «О защите персональных данных», направленный на внедрение всеохватывающего механизма защиты персональных данных, которые собираются, обрабатываются и/или хранятся любым физическим или юридическим лицом на территории Украины. Также с 09 мая вступили в силу Закон Украины «О доступе к публичной информации» и новая редакция Закона Украины «Об информации», принятые парламентом 13 января 2011 года. Указанные нормативно-правовые акты существенным образом изменили существующее правовое поле информационной деятельности в Украине, поэтому заслуживают внимания научного сообщества, юристов-практиков и широких кругов общественности.

По результатам проведенного обзора следует прийти к выводу, что представленный пакет «информационных законов» едва ли может служить достойной заменой предыдущей редакции Закона Украины «Об информации», которая носила комплексный характер. Продолжают существовать многочисленные коллизии между правом на информацию, правом доступа к информации и необходимостью обеспечивать неприкосновенность частной жизни, принципами информационной глобализации и необходимостью обеспечения безопасности информационного пространства. Такое состояние вещей будет сохраняться еще довольно долго и может быть исправлено лишь тогда, когда краеугольным камнем для разработки информационного законодательства станет именно информация (как объект правоотношений и цивилизационный феномен в условиях реализации концепции устойчивого развития), ее система и структура (в т.ч. четкое размежевание на виды и категории по режиму доступа), а также соответствующие права участников отношений, которые возникают в связи с информацией, и информационная безопасность.

LEGAL PRINCIPLES OF INFORMATIVE RELATIONS IN UKRAINE ARE NEW REALITIES

Darija Prokof'eva-Yanchilenko
Security of Ukraine Service

Since January 01, 2011 the Law of Ukraine «About protection of personal information», directed on introduction of the comprehensive mechanism of protection of personal information which are gathered, processed and/or stored by any physical or legal entity in Ukraine came into force. Also since May 09 came into force the Law of Ukraine «About access to public information» and new edition of the Law of Ukraine «About information», accepted by parliament on January 13, 2011. The specified normative legal acts essentially changed an existing legal framework of information activities in Ukraine therefore are worthy scientific community, experts lawyers ect.

By the results of the review it is necessary to come to a conclusion that the presented package of "information laws" hardly can serve as worthy replacement of the previous edition of the Law of Ukraine «About information» which had complex character. Numerous collisions between the right to information, right of access to information and need to provide inviolability of privacy, principles of information globalization and need of safety of information space continue to exist. Such situation will remain still long enough and can be corrected only when information (as object of legal relationship and a civilizational phenomenon in the conditions of implementation of the concept of sustainable development), its system and structure becomes a cornerstone for development of the information legislation (including accurate delimitation on types and categories on an access mode), and also the corresponding rights of participants of the relations which arise in connection with information, and information security.

УДК 004.77:340:347.121.1:347.121.2:

ОСОБЛИВОСТІ ПОРУШЕННЯ НЕМАЙНОВИХ ПРАВ ОСОБИ В ІНТЕРНЕТІ

Олександр Радкевич
Національна академія внутрішніх справ

Стаття: ***5 стор., 26 джерел.***

Зі створенням глобального інформаційного простору, основою якого є мережа Інтернет та інші системи передачі даних, актуальності набула проблема захисту у такому просторі немайнових прав осіб. Розміщення інформації персонального характеру в мережі Інтернет призводить до її видозмінення й перетворення на персональні дані. Правовий аспект персональної інформації обмежений територіальними рамками конкретної держави. Територіальна приналежність користувачів Інтернету неодмінно веде до зміни їх правого світогляду. Інтернет дає змогу встановлювати безпосередній контакт між людиною, яка перебуває під юрисдикцією однієї держави та, між різними суб'єктами інформаційного обміну, що перебувають на території інших держав. Так, складаються міжтериторіальний характер інформаційних відносин в мережі Інтернет. Порушення немайнових прав особи в Інтернеті виступає як неминучий наслідок стрімкого соціального розвитку, пов'язаного з ним прогресу чи регресу і зумовленого ними неузгодження соціального статусу індивіда. Суперечності між потребами й соціальними засобами їх задоволення, так само як і неузгодження статусу індивіда (освітнього, культурного), неминучі. Актуальність проблеми порушення немайнових прав особи в Інтернеті пов'язана із значним зростанням числа його споживачів. Згідно з останніми статистичними даними, у 2011 р. світова кількість споживачів Інтернет-послуг порівняно з 2000 р. зросла на 100%. Водночас збільшилася кількість випадків використання Інтернет-ресурсів у: кібершахрайстві, залякуванні, дискримінації, мережевому зломі, поширенні недостовірної інформації, втручання в особисте життя, сексуальні домагання за допомогою Інтернет-комунікацій, приниження гідності й честі, завдання шкоди діловій репутації, поширенні комп'ютерних вірусів тощо. До особистих немайнових прав належать: право на недоторканність особистого і сімейного життя; право на повагу честі, гідності та ділової репутації; право на свободу думки й слова та на вільне вираження своїх поглядів і переконань; право на особисте життя та його таємницю тощо. Для запобігання таких порушень в Інтернеті, як: хакерські атаки, підміна одержувача інформації (Man-in-the-Middle), поширенні комп'ютерних вірусів, перехоплення пакетів даних, добір паролів, технічний флуд тощо, необхідним є користування спеціальним програмним забезпеченням. До такого програмного забезпечення належать «Антивіруси», «Антивірусні сканери», «Антишпигуни», «Фаерволи» і подібні їм програми. З огляду на це актуалізується значення законодавчого регулювання відносин, що виникають під час використання мережі Інтернет.

ОСОБЕННОСТИ НАРУШЕНИЯ НЕИМУЩЕСТВЕННЫХ ПРАВ ЧЕЛОВЕКА В ИНТЕРНЕТЕ

Александр Радкевич
Национальная академия внутренних дел

С созданием глобального информационного пространства, основой которого является сеть Интернет и другие системы передачи данных актуальность приобрела проблема защиты неимущественных прав человека в таком пространстве. Размещение информации персонального характера в сети Интернет приводит к ее видоизменению и превращению в персональные данные. Правовой аспект персональной информации

ограничен территориальными рамками конкретного государства. Территориальная принадлежность пользователей Интернета непременно ведет к изменению их правого мировоззрения. Интернет позволяет устанавливать непосредственный контакт между человеком, который находится под юрисдикцией одного государства, и между различными субъектами информационного обмена, которые находятся на территории других государств. Так возникает межтерриториальный характер информационных отношений в сети Интернет. Нарушение неимущественных прав человека в Интернете выступает как неизбежное следствие социального развития, связанного с ним прогресса или регресса и обусловленного ими несогласованного социального статуса индивида. Противоречия между потребностями и социальными средствами их удовлетворения, равно как и несогласование статуса индивида (образовательного, культурного), неизбежны. Актуальность проблемы нарушения неимущественных прав человека в Интернете связана со значительным ростом количества его потребителей. Согласно последним статистическим данным, в 2011 г. мировое количество потребителей Интернет-услуг по сравнению с 2000 г. возросло на 100%. Одновременно участились случаи использования Интернет-ресурсов в кибермошенничестве, запугивании, дискриминации, сетевом взломе, распространении недостоверной информации, вмешательстве в личную жизнь, сексуальних домогательствах с помощью Интернет-коммуникаций, в унижение чести и достоинства, нанесение вреда деловой репутации, распространение компьютерных вирусов и т.д.. К личным неимущественным правам относятся: право на неприкосновенность личной и семейной жизни, право на уважение чести, достоинства и деловой репутации, право на свободу мысли и слова и на свободное выражение своих взглядов и убеждений, право на частную жизнь и его тайну и другие. Для предотвращения таких нарушений в Интернете, как: хакерские атаки, подмена получателя информации (Man-in-the-Middle), распространение компьютерных вирусов, перехват пакетов данных, подбор паролей, технический флуд и т.д., необходимо использование специального программного обеспечения. К такому програмному обеспечению относятся «Антивирусы», «Антивирусные сканеры», «Антишпионы», «Фаервол» и подобные им программы. Все это актуализирует значение законодательного урегулирования отношений, возникающих при использовании сети Интернет.

THE VIOLATION FEATURES OF INTANGIBLE RIGHTS PERSON ON THE INTERNET

Alexander Radkevich
National Academy of Internal Affairs

With the creation of a global information space, based on a network of Internet and other data transmission system has become actuality problem of protecting moral rights of persons in that space. Placing personal information in the nature of the Internet leads to modifying and converting to personal data. The legal aspect of personal information is limited territorial boundaries of each country. The territorial identity of Internet users will certainly lead to a change in their world outlook right. Internet allows to set the direct contact between a person who is under the jurisdiction of one country and between different subjects of the information exchange that are in other countries. So, there is inter–territorial nature of the information relationships in the Internet. Infringement of moral rights of individuals on the Internet acts as an inevitable consequence of social development and the related progress or regress and mismatches caused them social status of the individual. The contradictions between the needs and social means of meeting them, as well as the mismatch status of the individual (educational, cultural) are inevitable. Actuality of the problem of non-infringement of individual rights on the Internet is associated with a significant increase in the number of its customers. According to recent statistics in 2011, the world of consumer Internet-services compared to 2000 increased by 100%. At the same time increased the number of cases using the Internet-resources in cyber fraud, intimidation, discrimination, network hacking, distributing unreliable information, invasion of privacy, sexual harassments through the Internet-communication, dignity and honor humiliation, harm to reputation, spreading of viruses skinning coaxial and so on. To the private intangible rights include: right to privacy and family life, the right to respect for honor, dignity and business reputation, the right to freedom of thought and speech and free expression of views and beliefs, the right to privacy and his secrets and more. To prevent such violations on the Internet, as hackers, phishing recipient of the information (Man-in-the-Middle), spreading computer viruses, interception of data packets, the selection of passwords, technical flood, etc., it is necessary to use special software. Such software includes «Antivirus», «Anti-virus scanners», «Anti Spyware», «Firewall» and similar programs. Given this updated value of legislative regulation of relations arising when using the Internet.

УДК 651.928

ПОГЛЯД НА ПРАВОВУ ОСНОВУ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ ЗАКОНОТВОРЧОГО ПРОЦЕСУ

Роман Луценко
Національний технічний університет України "КПІ"

Стаття: ***5 стор., 11 джерел.***

За показниками кількості прийнятих законів Верховна Рада України вийшла на рівень парламентів розвинутих демократичних держав. Разом з тим, теорія і практика законотворчого процесу висувають численні вимоги щодо його вдосконалення як основного напряму розвитку сучасної правової системи України. Завдання вдосконалення законотворчої діяльності вимагає підняття на якісно новий щабель її наукового, нормативно-правового та організаційного забезпечення, у тому числі за напрямком вдосконалення чинного законодавства, яке регулює інформаційне забезпечення законодавчої процедури. Адже, нормативно-правове врегулювання відносин у вказаній сфері законотворчої діяльності ще не повною мірою відповідає вимогам практики. Значна нормативно-правова база у цій галузі (налічується майже 100 актів різної юридичної сили) складається з розгалуженого масиву нормативно-правових актів, які не здатні справляти цілісний правовий вплив на інформаційне забезпечення законотворчої діяльності. Проблема правового врегулювання пов'язана з тим, що розвиток інформаційного забезпечення законотворчого процесу відбувається у тісному взаємозв'язку зі світовими тенденціями, які пов'язані з становленням інформаційного суспільства, впровадженням нових інформаційних технологій, що стали істотним компонентом соціальної реальності й можуть розглядатися як фактор, що впливає на всі сфери життєдіяльності людини і суспільства.

ВЗГЛЯД НА ПРАВОВОЕ ОСНОВАНИЕ ИНФОРМАЦИОННОГО ОБЕСПЕЧЕНИЯ ЗАКОНОТВОРЧЕСКОГО ПРОЦЕССА

Роман Луценко
Национальный технический университет Украины "КПИ"

По показателям количества принятых законов Верховная Рада Украины вышла на уровень парламентов развитых демократических государств. Вместе с тем, теория и практика законотворческого процесса выдвигают многочисленные требования по его совершенствованию как основного направления развития современной правовой системы Украины. Задача совершенствования законотворческой деятельности требует поднятия на качественно новую ступень ее научного, нормативно-правового и организационного обеспечения, в том числе по направлению совершенствования действующего законодательства, регулирующего информационное обеспечение законодательной процедуры. Ведь, нормативно-правовое урегулирование отношений в указанной сфере законотворческой деятельности еще не полностью отвечает требованиям практики. Значительная нормативно-правовая база в этой области (насчитывается почти 100 актов различной юридической силы) состоит из разветвленного массива нормативно-правовых актов, которые не способны производить целостное правовое влияние на информационное обеспечение законотворческой деятельности. Проблема правового урегулирования связана с тем, что развитие информационного обеспечения законотворческого процесса происходит в тесной взаимосвязи с мировыми тенденциями, которые связаны со становлением информационного общества, внедрением новых информационных технологий, стали существенным компонентом социальной реальности и могут рассматриваться как фактор, что влияет на все сферы жизнедеятельности человека и общества.

A VIEW ON LEGAL BASIS OF INFORMATIONAL PROVIDING OF THE LEGISLATIVE PROCESS

Roman Lutsenko
National Technical University of Ukraine "KPI"

The number of laws adopted by Supreme Council of Ukraine corresponds to the level of developed democracies parliaments. At the same time, theory and practice of the legislative process impose numerous requirements concerning its improvement as the main direction of modern legal system of Ukraine development. The task of

legislative activity improving requires climbing to a qualitatively new level of its scientific, legal and organizational support, including improving the current legislation that regulates informational providing of the legislative procedure. In fact, legal regulation of relations in that sphere of legislative activity is not yet completely complies with the practice's requirements. Significant legislation in this field (there are about 100 various acts) consists of branched array of legal acts that are not able to make integral legal influence on the informational providing of the legislative activity. The problem of legal regulation related to the fact that informational providing of the legislative process development takes place in close interrelation with global trends related to the informational society development, introduction of new information technologies that have become an essential component of social reality.

УДК 004.056.5(045)

ОПТИМАЛЬНІ ФІНАНСОВІ ВИТРАТИ І ОСНОВНІ КРИТЕРІЇ ПОБУДОВИ АБО МОДЕРНІЗАЦІЇ КОМПЛЕКСУ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

Борис Журиленко, Надія Ніколаєва, Микита Пелих
Національний авіаційний університет

Стаття: ***11 стор., 7 джерел.***

При організації комплексу технічного захисту інформації (КТЗІ) в першу чергу цікавлять ефективність захисту і економічна вигода її застосування. Зі всіх можливих параметрів, визначаючих КТЗІ і зрозумілих для економічних розрахунків, є величини ризиків повних і вкладених в захист інформації фінансових втрат, вірогідність злому захисту при певній спробі злому і фінансові витрати на вибраний захист з даною вірогідністю злому. В результаті виконаної теоретичної роботи запропоновано метод розрахунку фінансових витрат при побудові або модернізації КТЗІ і метод розрахунку величини ризиків для повних фінансових втрат даного КТЗІ. Оптимізовані фінансові втрати у разі злому КТЗІ. Визначено критерій оптимізації витрат на побудову КТЗІ з урахуванням конкретних параметрів окремих захистів. В багаторівневому КТЗІ запропонований критерій визначає не тільки ефективність окремих захистів в КТЗІ, але і всього комплексу. Отримані вирази для розрахунку вірогідності злому як від величини вкладеного фінансування на захист інформації, так і від кількості спроб злому. Приведений вираз для розрахунку величини ризиків втрат фінансування, відповідній реальним системам захисту, параметри яких беруться з того або іншого захисту, що реально використовуються, тобто вірогідності злому для кожного захисту і реальним фінансовим витратам на їх організацію.

ОПТИМАЛЬНЫЕ ФИНАНСОВЫЕ ЗАТРАТЫ И ОСНОВНЫЕ КРИТЕРИИ ПОСТРОЕНИЯ ИЛИ МОДЕРНИЗАЦИИ КОМПЛЕКСА ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

Борис Журиленко, Надежда Николаева, Никита Пелих
Национальный авиационный университет

При организации комплекса технической защиты информации (КТЗИ) в первую очередь интересуют эффективность защиты и экономическая выгода ее применения. Из всех возможных параметров, определяющих КТЗИ и понятных для экономических расчетов, являются величины рисков полных и вложенных в защиту информации финансовых потерь, вероятность взлома защиты при определенной попытке взлома и финансовые затраты на выбранную защиту с данной вероятностью взлома. В результате выполненной теоретической работы предложены метод расчета финансовых затрат при построении или модернизации КТЗИ и метод расчета величины рисков для полных финансовых потерь данного КТЗИ. Оптимизированы финансовые потери в случае взлома КТЗИ. Определен критерий оптимизации расходов на построение КТЗИ с учетом конкретных параметров отдельных защит. В многоуровневом КТЗИ предложенный критерий определяет не только эффективность отдельных защит в КТЗИ, но и всего комплекса. Получены выражения для расчета вероятности взлома как от величины вложенного финансирования на защиту информации, так и от количества попыток взлома. Приведено выражение для расчета величины рисков потерь финансирования, соответствующие реальным системам защиты, параметры

которых берутся из реально используемой той или иной защиты, то есть вероятности взлома для каждой защиты и реальным финансовым затратам на их организацию.

OPTIMAL FINANCIAL COSTS AND MAIN CRITERIA OF CONSTRUCTION OR MODERNIZATION OF TECHNICAL INFORMATION SECURITY COMPLEX

Boris Zhurilenko, Nadezhda Nikolaeva, Nikita Pelikh
National Aviation University

The efficiency and economical benefits are the main focus in information technical protection complex (ITPC) arrangement. The size of full and information protection system included financial losses risks, described cracking attempt success probability and specified crack probability system cost are the most understandable and defining from all possible characteristics. As a result of theoretical research the ITPC development and upgrade cost calculation methods as well as full financial loss risks evaluation method for described system are suggested. The ITPC crack financial losses are optimized. The criteria of costs optimization is defined for ITPC development in consideration of separate protection's specific characteristics. In multilevel ITPC the suggested criteria defines not only the efficiency of separate protections in ITPC, but the whole complex efficiency. The crack probability evaluation formulas defined for financial investments in ITPC as well as for crack attempts quantity. The real protection systems corresponding risks values calculation formula is suggested, considering real systems characteristics, meaning each protection crack probability and real system arrangement financial costs.

УДК 621.396

СПОСІБ ДОСЛІДЖЕННЯ ПАРАМЕТРІВ ГОМОМОРФНОЇ ФУНКЦІЇ МОВНОГО СИГНАЛУ

Максим Кузнецов
Центр Інформаційно-аналітичних досліджень стратегічних програм

Стаття: ***7 стор., 4 джерел.***

Спектральний аналіз – це потужний та інформативних засіб дослідження складних сигналів але він потребує усереднювання спектральних складових, спрощення математичної моделі складних сигналів, що компроментує достовірність спектральних оцінок в аспекті визначення та зіставлення індивідуальних параметрів сигналів навіть для одного та й того же джерела. Розроблений новітній спосіб дослідження параметрів гомоморфної функції на основі квантилів (порядкових статистик) гомоморфної функції досліджуваних складних сигналів відноситься до області техніки автоматичної гомоморфної ідентифікації, селекції та розпізнавання джерел складних (мовних, гідроакустичних) сигналів. В умовах нестаціонарного характеру та великого динамічного діапазону змінення значень інтенсивності спектральних компонент складних сигналів, завдяки особливостям формування квантилів, відбувається нормалізація складових гомоморфної функції досліджуваних сигналів. Таким чином, у складі гомоморфного статистичного квантильного вектору складного сигналу, параметри гомоморфної функції набувають якостей стійкості до змінення як статистичних характеристик самого сигналу, так й статистичних характеристик каналів передавання сигналів. Значення гомоморфного статистичного квантильного вектору не усереднюються, реалізовано деталізацію векторів. Комплексне використання особливостей розробленого способу та пов'язаних з ними позитивних ефектів дозволяють забезпечити підвищення ефективності гомоморфної фільтрації складних сигналів.

СПОСОБ ИССЛЕДОВАНИЯ ПАРАМЕТРОВ ГОМОМОРФНОЙ ФУНКЦИИ РЕЧЕВОГО СИГНАЛА

Максим Кузнецов
Центр Информационно-аналитических исследований стратегических программ

Спектральный анализ - это мощные и информативное средство исследования сложных сигналов, но применение аппарата спектрального анализа предусматривает усреднение спектральных составляющих, упрощение математической модели сложных сигналов, что компрометирует достоверность спектральных оценок в аспекте определения и сопоставления индивидуальных параметров сигналов даже для одного и того же источника. Разработанный новый способ исследования параметров гомоморфной функции на основе квантилей (порядковых статистик) гомоморфной функции сложных сигналов относится к области техники автоматической гомоморфной идентификации, селекции и распознавания источников сложных (речевых, гидроакустических) сигналов. В условиях нестационарного характера и большого динамического диапазона изменений значений интенсивности спектральных компонент сложных сигналов, благодаря особенностям формирования квантилей, происходит нормализация составляющих гомоморфной функции исследуемых сигналов. Таким образом, в составе гомоморфного статистического квантильного вектора сложного сигнала, параметры гомоморфной функции приобретают качества стойкости к изменениям как статистических характеристик самого сигнала, так и статистических характеристик каналов передачи сигналов. Значение гомоморфного статистического квантильного вектора не усредняются, реализована детализация векторов. Комплексное использование особенностей разработанного способа и связанных с ними позитивных эффектов позволят обеспечить повышения эффективности гомоморфной фильтрации сложных сигналов.

THE METHOD OF RESEARCH OF SPEECH SIGNAL'S HOMOMORPHIC FUNCTION PARAMETERS

Maxim Kuznetsov
Centre of the Information and Analytics Researches of the Strategic Programs

Spectral analysis is a powerful and informative means of research of compound signals, but spectral analysis application provides the averaging of spectral components and simplification of mathematical model of compound signals, that compromises reliability of spectral estimations in the aspect of determining and comparing individual parameters even for one and the same source of the compound signal. The new method of the research of homomorphic function's parameters has been worked out. It is based on the usage of the quantiles (order statistics) of the parameters of the compound signal's homomorphic function and is referred to the area of methods of automatic homomorphic identification, selection and recognition of compound signals (vocal, hydroacoustic, etc.). Under the conditions of non-stationary character and wide dynamic range of values intensity of spectral components of compound signals, and due to the peculiarities of the quantiles' formation, the normalization of components of homomorphic function of the probed signals is taking place. Thus, in composition of the homomorphic statistical quantile vector of compound signal, the parameters of homomorphic function acquire the qualities of robustness to the changes of both statistical descriptions of signal and statistical descriptions of signals transmission channels. The homomorphic statistical quantile vector values are not averaged, the detailing of the statistical vectors components is implemented. Complex use of the features of the newly developed method and inherent positive effects allow to achieve the effectiveness of homomorphic filtration of compound signals.

УДК 681.3

МЕТОДИКИ ВИЗНАЧЕННЯ ЗАЛИШКОВИХ РИЗИКІВ У ЛОМ

Вячеслав Василенко
Національний авіаційний університет

Стаття: ***10 стор., 6 джерел.***

Для визначення вимог та оцінки захищеності інформації використовуються критерії оцінки захищеності. В статті пропонуються методики визначення кількісних показників захищеності інформації в ЛОМ – як величини залишкових ризиків. Розроблені методики, в яких пропонується для визначення кількісних показників захищеності використання ймовірностей: *порушення цілісності* – $q_{пц}$, *порушення конфіденційності* – $q_{пк}$, *порушення доступності* – $q_{пд}$ та *подолання, злому комплексної системи захисту* – q.

Оцінка по кожній із функціональних властивостей захищеності інформаційних ресурсів ЛОМ за методикою передбачає реалізацію наступних типових етапів:

1) побудова графічних моделей взаємодії загроз відповідній функціональній властивості захищеності інформаційних ресурсів ЛОМ із відповідними засобами захисту;

2) оцінка величин залишкових ризиків у ЛОМ;

3) визначення вихідних даних для оцінки залишкових ризиків у ЛОМ.

Аналіз зазначених у методіках виразів дозволяє зробити, перш за все, висновок про те, що:

- слабкість елементів системи захисту визначається найбільш слабкою ланкою цієї системи;
- для розрахунку відповідних ризиків можна виділити домінуючі ймовірності;
- усі змінні, які входять до складу виразів, що запропоновані для оцінки величин залишкових ризиків, можуть бути визначеними із застосуванням розроблених автором методик.

МЕТОДИКИ ОПРЕДЕЛЕНИЯ ОСТАТОЧНЫХ РИСКОВ В ЛВС

Вячеслав Василенко

Национальний авиационый университет

Для определения требований и оценки защищенности информации используются критерии оценки защищенности. В статье предлагаются методики определения количественных показателей защищенности информации в ЛВС – как величины остаточных рисков. Разработаны методики, в которых предлагается для определения количественных показателей защищенности использования вероятностей : нарушение целостности – $q_{пц}$, нарушения конфиденциальности – $q_{пк}$, нарушения доступности – $q_{пд}$ и преодоления, взлома комплексной системы защиты – q.

Оценка по каждой из функциональных свойств защищенности информационных ресурсов ЛВС по методике предусматривает реализацию следующих типичных этапов:

1) построение графических моделей взаимодействия угроз соответствующему функциональному свойству защищенности информационных ресурсов ЛВС с соответствующими средствами защиты;

2) оценка величин остаточных рисков в ЛВС;

3) определения выходных данных для оценки остаточных рисков в ЛВС.

Анализ отмеченных в методиках выражений позволяет сделать, прежде всего, вывод о том, что :

- слабость элементов системы защиты определяется наиболее слабым звеном этой системы;
- для расчета соответствующих рисков можно выделить доминирующие вероятности;
- все переменные, которые входят в состав выражений и предложены для оценки величин остаточных рисков, могут быть определены с применением разработанных автором методик.

THE METHODS OF DETERMINATION OF RESIDUAL RISKS IN LAN

Viacheslav Vasilenko

National aviation university

To determine the requirements and evaluation of information security evaluation criteria used by security. The article proposes methods for determining quantitative information security in a LAN as the quantities of residual risks. Methods have been developed, which is proposed for quantifying the probability of protection: $q_{пц}$ - violation of the integrity,violation of confidentiality - $q_{пк}$, $q_{пд}$ - violation accessibility and overcome, cracking the complex security system - q.

Score each of the functional properties of the security of information resources on the LAN procedure sets forth the following typical steps:

1) the construction of graphical interaction models threats the corresponding functional property information resources security LAN with appropriate protective equipment;

2) evaluation of the quantities of residual risks in the LAN;

3) determination of the output data to assess the residual risks on the LAN.

The analysis noted in the methods of expressions allows us to, first of all, the conclusion that:

- Weakness of the elements of the system of protection is determined by the weakest link in the system;
- To calculate the risks involved can be identified dominating probability;
- All variables that are part of the expressions and proposed to assess the quantities of residual risks can be identified using techniques developed by the author.

УДК 004.056.5(045)

БЕЗПЕКА ПРИ ПЕРЕНЕСЕННІ ДАНИХ НА ІНШУ ОПЕРАЦІЙНУ СИСТЕМУ

Сергій Єгоров
Національний авіаційний університет

Статя: ***5 стор., 6 джерел.***

У зв'язку з різким зростанням в повсякденному житті електронного документообігу і впливом інформаційних воєн на електронну документацію питання про безпечний перехід на іншу операційну систему (ОС) і безпечне резервне копіювання стає дуже актуальним. Метою даної статті є розробка рекомендацій для здійснення безпечного переходу зі старшої версії ОС Windows на іншу, молодшу.

Резервне копіювання актуально не тільки в процесі експлуатації ОС, але і при переході на нову ОС. При першій установці нової ОС доцільно створити резервну копію ОС, відразу після того, як ви встановите на неї все програмне забезпечення, яке ви використовуєте, разом з драйверами.

Слід виконувати резервне копіювання тих файлів, які важко або неможливо замінити або якщо файл часто змінюється. Кандидатами на резервне копіювання можуть бути наступні файли: малюнки, цифрові фотографії, відео, фінансові документи, проекти.

Не слід виконувати резервне копіювання тих програм, які зазвичай займають багато дискового простору, так як їх можна відновити, скориставшись дисками оригінальних продуктів для повторної установки.

БЕЗОПАСНОСТЬ ПРИ ПЕРЕНОСЕ ДАННЫХ НА ДРУГУЮ ОПЕРАЦИОННУЮ СИСТЕМУ

Сергей Егоров
Национальный авиационный университет

В связи с резким ростом в повседневной жизни электронного документооборота и влиянием информационных войн на электронную документацию вопрос о безопасном переходе на другую операционную систему (ОС) и безопасном резервном копировании становиться очень актуальным. Постановка задачи : целью данной статьи является разработка рекомендаций для осуществления безопасного перехода со старшей версии ОС Windows на другую, младшую.

Резервное копирование актуально не только в процессе эксплуатации ОС, но и при переходе на новую ОС. При первой установке новой ОС целесообразно создать резервную копию ОС, сразу после того, как вы установите на неё всё программное обеспечение, которое вы используете, вместе с драйверами.

Следует выполнять резервное копирование тех файлов, которые трудно или невозможно заменить или если файл часто изменяется. Кандидатами на резервное копирование могут быть следующие файлы: рисунки, цифровые фотографии, видео, финансовые документы, проекты.

Не следует выполнять резервное копирование тех программ, которые обычно занимают много дискового пространства, так как их можно восстановить, воспользовавшись дисками оригинальных продуктов для повторной установки.

SECURITY WHILE TRANSFERING DATA TO ANOTHER OPERATING SYSTEM

Serhii Yehorov
National aviation university

Due to the sharp increase in the daily life of electronic documents and information warfare influence on the electronic records issue of safe passage to another operating system (OS) and the safe backing up to become very important. Problem Statement: The goal of this paper is to develop recommendations for a safe transition from an older version of Windows to another, younger.

Backing up important not only during the operation running, but the transition to the new OS. When you first install the new OS it is advisable to back up the OS as soon as you install it on all the software you use, along with the drivers.

It should be back up those files that are difficult or impossible to replace, or if the file changes frequently. Candidates for the backup may be the following files: pictures, digital photos, video, financial documents, projects.

You should not back up those programs, which usually take a lot of disk space, since they can be restored using the original discs to reinstall the product.

УДК 004.932 : 621.391.7

СПОСІБ СТЕГАНОГРАФІЇ ЗОБРАЖЕНЬ З ФРАГМЕНТАЦІЄЮ СТЕГОДАНИХ ТА РОЗДІЛЕННЯМ ЗАКРИТОГО КЛЮЧА

Євгенія Сулема, Семен Широчин
НТУУ «КПІ», Факультет прикладної математики

Стаття: ***5 стор, 5 джерел.***

На сьогоднішній день існує багато методів захисту інформації, в тому числі й таких, що ґрунтуються на стеганографії. Але оскільки методи стегоаналізу постійно вдосконалюються, то задача створення нових способів стеганографічного захисту інформації є та буде залишатись актуальною. В статті пропонується спосіб, який відноситься до стеганографії простору зображень та ґрунтується на розміщенні стегоданих у найменш значущих бітах (LSB) з використанням спеціального алгоритму фрагментації. Спосіб передбачає утворення закритого ключа, що може бути розділений на частини для збереження та передачі їх окремо від контейнеру. Ключ складається з вектору початкових адрес та вектору довжин фрагментів. В статті розглядаються основні засади LSB-стеганографії та формулюються вимоги до алгоритму фрагментації стегоданих, що лежить в основі запропонованого способу. В основній частині статті автори наводять схему стеганографічного перетворення, алгоритм фрагментації стегоданих, алгоритм відновлення стегоданих та формули розрахунку адрес для алгоритму фрагментації. В якості контейнеру пропонується використовувати графічні файли формату PNG, оскільки даний формат передбачає ущільнення графічних даних без втрат. Алгоритм стеганографічного перетворення з фрагментацією стегоданих та алгоритм без фрагментації стегоданих були реалізовані програмним шляхом для порівняльної оцінки їх швидкодії. В статті наведено експериментальні дані щодо часу роботи обох алгоритмів для різних контейнерів та зображень (стегоданих). Отримані дані показують, що використання фрагментації незначно збільшує час роботи алгоритму. Це дозволяє зробити висновок про можливість застосування запропонованого способу стеганографії зображень з фрагментацією стегоданих та розділенням закритого ключа на практиці.

СПОСОБ СТЕГАНОГРАФИИ ИЗОБРАЖЕНИЙ С ФРАГМЕНТАЦИЕЙ СТЕГОДАННЫХ И РАЗДЕЛЕНИЕМ ЗАКРЫТОГО КЛЮЧА

Евгения Сулема, Семён Широчин
НТУУ «КПИ», Факультет прикладной математики

На сегодняшний день существует много методов защиты информации, в том числе и таких, которые основываются на стеганографии. Поскольку методы стегоанализа постоянно совершенствуются, то задача создания новых способов стеганографической защиты информации является и будет оставаться актуальной. В статье предлагается способ, который относится к стеганографии пространства изображений и основывается на размещении стегоданных в наименее значимых битах (LSB) с использованием специального алгоритма фрагментации. Способ предусматривает создание закрытого ключа, который может быть разделен на части для хранения и передачи их отдельно от контейнера. Ключ состоит из вектора начальных адресов и вектора длин фрагментов. В статье рассматриваются основные принципы LSB-стеганографии и формулируются требования к алгоритму фрагментации стегоданных, который лежит в основе предложенного способа. В основной части статьи авторы приводят схему стеганографического преобразования, алгоритм фрагментации стегоданных, алгоритм восстановления стегоданных и формулы расчета адресов алгоритма фрагментации. В качестве контейнера предлагается использовать графические файлы формата PNG, так как данный формат предусматривает сжатие графических данных без потерь. Алгоритм стеганографического преобразования с фрагментацией стегоданных и алгоритм без фрагментации стегоданных были реализованы программным путем для сравнительной оценки их быстродействия. В статье приведены экспериментальные данные о времени работы обоих алгоритмов для различных контейнеров и

изображений (стегоданных). Полученные данные показывают, что использование фрагментации незначительно увеличивает время работы алгоритма. Это позволяет сделать вывод о возможности практического применения предложенного способа стеганографии изображений с фрагментацией стегоданных и разделением закрытого ключа.

The METHOD OF IMAGE DOMAIN STEGANOGRAPHY WITH STEGODATA FRAGMENTATION AND SEPARATION OF PRIVATE KEY

Yevgeniya Sulema, Semen Shyrochyn
National Technical University of Ukraine "KPI"

Nowadays there is a significant number of data security methods, including the methods which are based on steganography. However, since stegoanalysis methods are improving continually, the task of the development of new methods for steganography data protection is and will remain topical. The method relates to image domain steganography and based on less significant bit (LSB) stegodata allocation with special fragmentation algorithm is proposed in this article. The method implies a separable private key to keep it separately from the container. The key consists of initial addresses vector and fragment lengths vector. The fundamentals of LSB-steganography as well as the demands to stagodata fragmentation algorithm are discussed in the article. In the main part of the article the authors present the schema of steganography transform, stegodata fragmentation algorithm, and formulas for addresses calculation in the fragmentation algorithm. Graphical files in PNG format are proposed to be used as container, because this format supports lossless compression of graphical data. Both the algorithm of steganography transform with stegodata fragmentation and the algorithm without stagodata fragmentation have been realized as software applications in order to estimate and compare their processing speed. The experimental data for performance time of both algorithms for different containers and images (stegodata) are given in the article. The obtained data indicate that the fragmentation increases the time of the algorithm performance inconsiderably. This fact allows to conclude that the proposed method of image domain steganography with stegodata fragmentation and separation of private key can be applied in practice.

УДК 006.86(045)

НОВІТНІ ПРИНЦИПИ ДОСЯЖНОСТІ ЯКОСТІ ЛАБОРАТОРНИХ ВИПРОБУВАНЬ. СТАТИСТИЧНИЙ ПІДХІД лваолва

Лариса Кошева
Національний авіаційний університет

Стаття: ***11 стор., 11 джерел.***

Для забезпечення високої якості результатів випробувань та забезпечення їх порівнянності незалежно від місця та часу їх проведення необхідно застосовувати сучасні підходи до організації та проведення випробувального процесу, в основу яких покладено статистичні методи. Статистичні методи можуть сприяти кращому розумінню плину, строків та причин мінливості, що впливає на результати, навіть за наявності обмеженого статистичного матеріалу, а в подальшому – при вирішенні і навіть попередженні проблем, пов'язаних з такого роду мінливістю. Складові випробувального процесу, що впливають на якість результату (методика, випробувальне обладнання, умови, оператор) утворюють систему забезпечення якості, що побудована на основі статистичного підходу, який застосовується при встановленні характеристик точності методик випробувань та оцінюванні результатів випробувань, отриманих при їх реалізації; встановленні придатності стандартизованих методик; оцінюванні прийнятності результатів випробування; оцінюванні професійного рівня лабораторій; підтриманні процесу одержання результатів випробувань на заданому рівні; формуванні співдружності лабораторій, що виконують випробування у певній галузі; встановленні метрологічних характеристик лабораторії з урахуванням індивідуальних особливостей та відмінностей організації випробувального процесу в них, що не мають кількісної оцінки, та урахуванні їх при оцінюванні результатів, отриманих у лабораторії. Показано, що зіставлення отриманих результатів засновані не на виявленні різниці між двома дисперсіями або між двома середніми значеннями, а на застосуванні критеріїв

статистичної значущості, що використовують поняття приналежності результатів випробувань до одної або різних множин.

НОВЕЙШИЕ ПРИНЦИПЫ ДОСЯГАЕМОСТИ КАЧЕСТВА ЛАБОРАТОРНЫХ ИСПЫТАНИЙ. СТАТИСТИЧЕСКИЙ ПОДХОД

Лариса Кошева
Национальный авиационный университет

Для обеспечения высокого качества результатов испытаний и обеспечения их сопоставимости независимо от места и времени их проведения необходимо применять современные подходы к организации и проведению испытательного процесса, в основе которых положены статистические методы. Статистические методы могут содействовать лучшему пониманию течения, сроков и причин изменчивости, влияющей на результаты, даже при наличии ограниченного статистического материала, а в дальнейшем – при решении и даже предотвращении проблем, связанных с такого рода изменчивостью. Составляющие испытательного процесса, влияющие на качество результата (методика, испытательное оборудование, условия, оператор) образуют систему обеспечения качества, основанную на статистическом подходе, который применяется для установления характеристик точности методик испытаний и оценке их результатов; установления пригодности стандартизированных методик; оценки приемлемости результатов испытания; оценки профессионального уровня лабораторий; поддержания процесса получения результатов испытаний на заданном уровне; формирования содружества лабораторий, выполняющих испытания в определенной области; установления метрологических характеристик лаборатории с учетом индивидуальных особенностей и различий в организации испытательного процесса в них, не имеющих количественной оценки, и учета их при оценке результатов, полученных в лаборатории. Показано, что сопоставление полученных результатов основано не на выявлении различий между двумя дисперсиями или между двумя средними значениями, а на применении критериев статистической значимости, использующих понятие принадлежности результатов испытаний к одному или разным множествам.

THE NEWEST PRINCIPLES OF REACH OF QUALITY OF ALPHA TESTS. THE STATISTICAL APPROACH

Larysa Kosheva
National aviation university

Currently, to ensure high quality test results and make them comparable, regardless of location and time of their need to apply modern approaches to the organization and conduct of the trial process, which are based on statistical methods. Statistical methods can contribute to a better understanding of the flow, timing and causes of variability affecting the results, even with limited statistical material, and in the future – in the solution and even prevention of problems associated with such variability.Components of the test process, affecting the quality of results (method, test equipment, conditions, operator) form a quality assurance system based on a statistical approach, which is used to determine the characteristics of the accuracy of testing methods and evaluating their results, the suitability of standardized methods, for assessing the acceptability of test results; assessment of professional-level laboratories to support the process of obtaining the test results at a given level, the formation of the commonwealth of laboratories performing tests in a particular area; establishing the metrological characteristics of the laboratory, taking into account individual characteristics and differences in the organization of the trial process in them, without quantifying, and recording their when evaluating the results obtained in the laboratory. It is shown that a comparison of the results is not based on the identification of differences between two variances, or between two averages, and the application of the criteria of statistical significance, using the concept of membership of the test results to the same or different sets.

УДК 531/534(075.8)

ОПТИМІЗАЦІЯ ХАРАКТЕРИСТИК РАДІОЕЛЕКТРОННИХ ЗАСОБІВ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

Борис Уваров, Юрій Зіньковський

Національний технічний університет України "Київський політехнічний інститут"

Стаття: ***8 стор., 4 джерел.***

Одним з найважливіших показників призначення радіоелектронних засобів (РЕЗ) технічного захисту інформації (ТЗІ) є надійність, оскільки будь-яка відмова (непрацездатність) якої-небудь структурної одиниці комплексу ТЗІ може привести або до просочування інформації за межі контрольованої зони, або до зовнішнього впливу на систему, де інформація створюється, обробляється, накопичується або зберігається.

Значення показників надійності таких РЕЗ мають бути максимально високими, а можливості і засоби для їх досягнення необхідно передбачати вже при проектуванні на стадії створення структурної моделі майбутнього РЕЗ. Найвищі показники якості РЕЗ досягаються параметричною оптимізацією всіх або більшості вихідних параметрів моделі. Після формування структурної моделі проектують структурні складові всього РЕЗ і визначають їх конструктивні параметри, а також розраховують основні функціональні характеристики пристрою. Це дає можливість розрахувати значення всіх одиничних, часткових і комплексного критерію $\overline{K}$.

Для досягнення найвищих показників якості необхідно послідовними ітераціями провести параметричну оптимізацію зміною значень первинних величин і це дозволяє підвищити стійкість РЕЗ до зовнішніх механічних дій, повністю зберігаючи спочатку вибрані форму і розміри елементів конструкції, застосовані для них матеріали.

Основними об'єктами оптимізації в РЕЗ мають бути структурно-конструктивні модулі першого порядку (СКМ1) – т.з. вічка і МСб – функціонально закінчені РЕЗ, які розміщені на пластмасовій, металевій або керамічній друкованій платі. У загальному об'ємі різноманітних РЕЗ СКМ1 складають не менше 67–85% структурних елементів і тому можна вважати, що саме вони і повинні розглядатися як основні об'єкти, показників конструктивної і функціональної досконалості яких необхідно досягти в першу чергу. Для них і повинні перш за все створюватися методи проектування оптимальних конструкцій.

Чисельним моделюванням показано, що раціональна компоновка елементів на друкованій платі або підложці мікрозборки може у ряді випадків підвищити вірогідність безвідмовної роботи РЕЗ при механічних впливах на 45 – 50%, а при теплових – на 20 – 35%. В результаті параметричної оптимізації топології конструктивних модулів з вказаними елементами буде отримана і максимальна надійність конструкції РЕЗ.

ОПТИМИЗАЦИЯ ХАРАКТЕРИСТИК РАДИОЭЛЕКТРОННЫХ СРЕДСТВ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

Борис Уваров, Юрий Зиньковский

Национальный технический университет Украины "Киевский политехнический институт"

Одним из важнейших показателей назначения радиоэлектронных средств (РЭС) технической защиты информации (ТЗИ) является надежность, т. к. любой отказ (неработоспособность) какой-либо структурной единицы комплекса ТЗИ может привести или к утечке информации за пределы контролируемой зоны, или к внешнему воздействию на систему, где информация создается, обрабатывается, накапливается или хранится. Значение показателей надежности таких РЭС должны быть максимально высокими, а возможности и средства для их достижения необходимо предусматривать уже при проектировании на стадии создания структурной модели будущего РЭС. Наивысшие показатели качества РЭС достигаются параметрической оптимизацией всех или большинства исходных параметров модели.

После формирования структурной модели проектируют структурные составляющие всего РЭС и определяют их конструктивные параметры, а также рассчитывают основные функциональные характеристики устройства. Это дает возможность рассчитать значения всех единичных, частичных и комплексного критерия $\overline{K}$.

Для достижения наивысших показателей качества необходимо последовательными итерациями провести параметрическую оптимизацию изменением значений первичных величин и это позволяет повысить

стойкость РЭС к внешним механическим воздействиям, полностью сохраняя первоначально выбранные форму и размеры элементов конструкции, примененные для них материалы.

Основными объектами оптимизации в РЭС должны быть структурно-конструктивные модули первого порядка (СКМ1) – т.н. ячейки и МСб – функционально законченные РЭС, которые размещены на пластмассовой, металлической или керамической печатной плате (ПП). В общем объеме всей разнообразной РЭС СКМ1 составляют не менее 67–85% структурных элементов, поэтому можно считать, что именно они и должны рассматриваться как основные объекты, показателей конструктивного и функционального совершенства которых необходимо достичь в первую очередь. Для них и должны прежде всего создаваться методы проектирования оптимальных конструкций.

Численным моделированием показано, что рациональная компоновка элементов на основании печатной платы или подложки микросборки может в ряде случаев повысить вероятность безотказной работы РЭС при механических воздействиях на 45 – 50%, а при тепловых – на 20 – 35%. В результате параметрической оптимизации топологии конструктивных модулей с указанными элементами будет получена и максимальная надежность конструкции РЭС.

OPTIMAZATION OF CHARACTERISTICS OF RADIO ELECTRONIC TECHNICAL INFORMATION SECURITY PRODUCTS

Boris Uvarov, Yuriy Zinkovsky
National Technical University of Ukraine "Kyiv Polytechnic Institute"

One of the most important indicators of use of electronic means (RECs), technical protection of information (TZI) is reliable, because any failure (non-functional), a structural unit of complex proofing may or may leak information outside the controlled area, or to external influence on a system where information is created, processed, stored or kept. The value of reliability of the RECs should be as high as possible and the means to achieve them must be provided even at the design stage to create a structural model of the future RECs. The highest quality is achieved RES parametric optimization of all or most of the initial parameters of the model.

After the formation of a structural model of designing structural components of the RECs and determine their structural parameters and calculate the key features of the device. This makes it possible to calculate the values $\overline{K}$ of all single, partial and complex criteria.

To achieve the highest quality to successive iterations to optimize the parametric variation of the primary values of variables and it allows to increase the resistance of RES to external mechanical influences, while maintaining the original shape and size of the selected design elements that are applied to these materials. The main objects of optimization in the RES must be structural and structural units of the first order (SKM1) - the so-called cells and SMEs - a functionally complete RECs, which are placed on a plastic, metal or ceramic printed circuit board (PCB). In total across a variety of RES SKM1 is at least 67-85% of the structural elements, so we can assume that they, and should be considered as basic objects, constructive and functional parameters of perfection to be achieved in the first place. For them, and must first be established methods of design of optimal structures.

Numerical simulation shows that the rational layout of elements on the basis of the printed circuit board or substrate micro can, in some cases increase the probability of failure of RES by mechanical action on 45 - 50%, and with heat - 20 - 35%. As a result, the parametric optimization of structural topology of the modules with the above elements will be obtained and maximum reliability of the design RES.

УДК 621.395

ВПЛИВ ЗМІНИ СТРУКТУРИ ВІДОМЧИХ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ НА ЗАБЕЗПЕЧЕННЯ ЗАДАНИХ ЗНАЧЕНЬ ПОКАЗНИКІВ ЯКОСТІ ОБСЛУГОВУВАННЯ

Дмитро Могилевич, Валерій Правило, Олександр Захараш
ВІТІ НТУУ "КПІ"

Стаття: ***6 стор., 5 джерел.***

Розглянуті питання виконання значень імовірності безвідмовного обслуговування заявок на телекомунікаційних мережах (ТКМ). Одним із шляхів вирішення даної задачі є введення в структуру мережі додаткових гілок. В статті наведено розрахунки, отримані методом сукупності шляхів або перетинів. Надано графіки залежності значень імовірності безвідмовного обслуговування додаткових перемичок в структурі мережі від імовірності безвідмовного обслуговування гілок, що становлять шляхи встановлення з'єднання.

Характеристика, що визначає можливість абонентів обмінюватися інформацією мережами зв'язку в умовах виникнення технічних відмов й експлуатаційних помилок на її елементах без помітного погіршення імовірнісно-часових показників обслуговування заявок одержала назву надійності функціонування мереж зв'язку. Тому під надійністю функціонування мережі зв'язку розуміється її властивість забезпечувати встановлення з'єднань і передачу повідомлень у реальних умовах експлуатації при збереженні значень показників якості обслуговування, встановленого для кожного напрямку зв'язку. Показником якості обслуговування заявок у напрямку зв'язку ТКМ, що може бути розглянута як n-канальна система масового обслуговування з відмовами або з очікуванням, прийнято вважати ймовірність безвідмовного обслуговування

Мета даної роботи – визначити можливі шляхи забезпечення заданого значення ймовірності безвідмовного обслуговування заявок в обраному напрямку зв'язку й на ТКМ у цілому шляхом змінювання (нарощування) структури мережі в умовах виходу з ладу (відмови) її елементів внаслідок технічних відмов, сторонніх впливів, стихійних явищ тощо.

ВЛИЯНИЕ ИЗМЕНЕНИЯ СТРУКТУРЫ ВЕДОМСТВЕННЫХ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ НА ОБЕСПЕЧЕНИЕ ЗАДАННЫХ ЗНАЧЕНИЙ ПОКАЗАТЕЛЕЙ КАЧЕСТВА ОБСЛУЖИВАНИЯ

Дмитрий Могилевич, Валерий Правило, Александр Захараш
ВИТИ НТУУ "КПІ"

Рассмотрены вопросы выполнения значений вероятности безотказного обслуживания заявок на телекоммуникационных сетях (ТКС). Одним из путей решения данной задачи является введение в структуру сети дополнительных ветвей. В статье приведены расчеты, полученные методом совокупности путей или сечений, и графики зависимости значений вероятности безотказного обслуживания дополнительных перемычек в структуре сети от вероятности безотказного обслуживания ветвей, которые представляют пути установления соединения.

Характеристика, которая определяет возможность абонентов обмениваться информацией по сетям связи в условиях возникновения технических отказов и эксплуатационных ошибок на ее элементах без заметного ухудшения вероятностно-временных показателей обслуживания заявок получила название надежности функционирования сетей связи. Поэтому под надежностью функционирования сети связи понимается ее свойство обеспечивать установление соединений и передачу сообщений в реальных условиях эксплуатации при сохранении значений показателей качества обслуживания, установленного для каждого направления связи. Показателем качества обслуживания заявок в направлении связи ТКС, которая может быть рассмотрена как n-*канальная* система массового обслуживания с отказами или с ожиданием, принято считать вероятность безотказного обслуживания.

Целью данной работы является определение возможных путей обеспечения заданного значения вероятности безотказного обслуживания заявок в выбранном направлении связи и на ТКС в целом путем изменения (наращивания) структуры сети в условиях выхода из строя (отказа) ее элементов вследствие технических причин, посторонних влияний, стихийных явлений и т. д.

THE INFLUENCE OF CHANGE OF STRUCTURE OF DEPARTMENTAL TELECOMMUNICATION NETWORKS ON SUPPORT OF SETTING VALUATIONS QUALITY OF SERVICE

Dmitro Mogilevich, Valeriy Pravilo, Oleksandr Zaharash
MITI NTUU "KPI"

In article questions of performance of values of probability fault-free upkeeps of requests on telecommunication

networks (TCN) are considered. One of ways of the decision of the given task is introduction in structure of a network of additional branches. In article the calculations received by a method of set of ways or sections are resulted. Schedules of dependence of values of probability fault-free upkeeps of additional jumpers in structure of a network from probability fault-free upkeeps of branches which represent connection establishment ways are given.

The characteristic which defines possibility of subscribers to communicate on communication networks in the conditions of origin of technical failures and operational errors on its elements without noticeable impairment of is probability-time indexes of service of requests, received a title of reliability of functioning of communication networks. Therefore reliability of functioning of a communication network is understood as its property to provide establishment of connections and message transfer in actual practice maintenance at saving of values of quality characteristics of the service installed for each direction of communication. In a direction of communication TCN which can be considered as n-channel system of mass service with failures or with waiting, it is considered to be a quality characteristic of service of requests probability fault-free upkeeps.

The aim of the given operation puts determination of possible ways of support of a preset value of probability fault-free upkeeps of requests in the selected direction of communication and on TCN as a whole by change (escalating) of structure of a network, in the conditions of failure of its elements owing to the technical reasons, outside influences, the spontaneous phenomena etc.

УДК 35.078:342.738

НАЛАШТУВАННЯ ЗАХИСНИХ ВЛАСТИВОСТЕЙ БОКСУ ДЛЯ МОБІЛЬНИХ ТЕЛЕФОНІВ

Владислав Черниш, Ігор Жуков
Харківський національний університет радіоелектроніки

Стаття: ***5 стор, 6 джерел.***

Розглянуті основні захисні властивості захисного боксу для мобільних телефонів. У роботі представлені дослідження рівня звукоізоляції захисного боксу на частотах мовного сигналу. Результати досліджень можна використати для захисту мовної конфіденційної інформації.

Забезпечення конфіденційності мовної інформації є актуальним питанням у галузі безпеки інформації. При проведенні нарад, конференцій, засідань власник інформації з обмеженим доступом (ІзОД) стикається з проблемою можливості її витоку через закладний пристрій, який може бути вбудований або запрограмований у мобільний телефон без відома власника телефону. Прийняті способи захисту від такого каналу витоку: залишення мобільного телефону за межами виділеного приміщення або вимкнення телефону із обов'язковим вийманням батарей живлення із нього. Обидва способи натикаються на спротив їх власників, обумовлений, перш за все, тимчасовою втратою зв'язку.

Подолання вказаних недоліків: 1) запобігання витоку мовної через закладний пристрій мобільного телефону, 2) забезпечення оптичної та звукової індикації виклику власника телефону може бути забезпечено за допомогою захисного боксу для мобільних телефонів.

НАСТРОЙКИ ЗАЩИТНЫХ СВОЙСТВ БОКСа ДЛЯ МОБИЛЬНЫХ ТЕЛЕФОНОВ

Владислав Черныш, Игорь Жуков
Харьковский национальный университет радиоэлектроники

Рассмотрены основные защитные свойства защитного бокса для мобильных телефонов. В работе представлены исследования уровня звукоизоляции защитного бокса на частотах речевого сигнала. Результаты исследований можно использовать для защиты речевой конфиденциальной информации.

Обеспечение конфиденциальности речевой информации является актуальным вопросом в области безопасности информации. При проведении совещаний, конференций, заседаний владелец информации с ограниченным доступом (ИсОД) сталкивается с проблемой возможности ее утечки через закладные устройства, который может быть встроен или запрограммированный в мобильный телефон без ведома владельца телефона. Принятые способы защиты от такого канала утечки: оставление мобильного телефона за пределами выделенного помещения и выключение телефона с обязательным извлечением батарей питания

из него. Оба способа натыкаются на сопротивление их владельцев, обусловлен, прежде всего, временной потерей связи.

Преодоление указанных недостатков: 1) предотвращение утечки речевой через закладные устройства мобильного телефона, 2) обеспечение оптической и звуковой индикации вызова владельца телефона может быть обеспечено с помощью защитного бокса для мобильных телефонов.

SETTINGs of THE PROTECTIVE PROPERTIES OF BOXING FOR MOBILE PHONES

Vladislav Chernish, Ihor Zhukov
Kharkov National University of Radioelectronics

The main protective properties of protective boxing for mobile phones are observed. The work presents the research level of soundproofing protective boxing at frequencies of speech signal. The research results can be used to protect privacy voice data.

Ensuring confidentiality of voice information is relevant to the security of information. While conducting meetings, conferences, owner of the information with restricted access (IsOD) faced with the possibility of leakage through eavesdropping devices, which can be embedded or programmed in the mobile phone without your knowledge. Accepted methods of protection against leakage of such a channel: the abandonment of mobile phone outside the selected area on or off with the obligatory removing batteries from it. Both methods run into resistance of their owners, is due, above all, a temporary loss of communication.

Overcoming these shortcomings: 1) prevention of leakage of audio eavesdropping devices through the mobile phone, 2) provide visual and audible indication of the owner of the phone call may be provided with protective housings for mobile phones.

УДК 534.21:004.56.5(045)

АКУСТИЧНА СИСТЕМА АДАПТИВНОГО ПРИГНІЧЕННЯ ІНФОРМАТИВНОГО СИГНАЛУ

Ростислав Сазонов, Борис Журиленко
Націоанальний авіаційний університет

Стаття: ***7 стор., 5 джерел.***

Системи адаптивного пригнічення звукового сигналу можна спробувати застосувати для захисту акустичної інформації в приміщенні. При цьому в межах охоронної зони за допомогою компенсуючих акустичних систем створюється область, за межами якої рівень звуку або відсутній, або значно ослабляється, або спотворюється до стану, який не можливо розпізнать. Тому представляє інтерес дослідження просторового розподілу поля звукової хвилі від джерел інформації і акустичних систем компенсації поля хвилі. Для досягнення поставленої мети використовувалося електронно-обчислювальне середовище Mathcad, в якому було змодельовано завдання просторового розподілу поля звукової хвилі від N- джерел інформації і N- акустичних систем компенсації поля хвилі. Аналізуючи отримані результати, можна зробити висновок про можливість створення акустичної системи адаптивного пригнічення інформаційного сигналу, але для певних умов.

Для усіх розглянутих частот в центрі розподілу потужності компенсації випромінювань спостерігається область з досить низьким рівнем випромінювання, оточена більш високими амплітудними складовими, що дає можливість використання цієї зони для ведення, наприклад, захищених переговорів. Така система може виявитися найбільш ефективною і простою щодо технічної реалізації захисту інформації за умови створення сферичної хвилі як від джерела інформації (людини), так і компенсуючої акустичної системи.

Що ж до створення системи захисту від витоку по акустичному каналу при поширенні плоских затухаючих і плоских незгасаючих хвиль, то зроблений висновок, що для цієї ситуації, коли є 2 джерела інформаційного сигналу і 2 акустичних пригнічуючих системи, реалізація захисту неможлива. В цьому випадку слід припустити, що для захисту необхідно використати більшу кількість акустичних систем з певною амплітудою, розташованих на певній відстані.

АКУСТИЧЕСКАЯ СИСТЕМА АДАПТИВНОГО ПОДАВЛЕНИЯ ИНФОРМАЦИОННОГО СИГНАЛА

Ростислав Сазонов, Борис Журиленко
НАЦИОНАЛЬНЫЙ АВИАЦИОННЫЙ УНИВЕРСИТЕТ

Системы адаптивного подавления звукового сигнала можно попытаться применить для защиты акустической информации в помещении. При этом в пределах охранной зоны с помощью компенсирующих акустических систем создается область, за пределами которой уровень звука либо отсутствует, либо значительно ослабляется, либо искажается до неразборчивого состояния. Поэтому представляет интерес исследование пространственного распределения поля звуковой волны от источников информации и акустических систем компенсации поля волны. Для достижения поставленной цели использовалась электронно-вычислительная среда Mathcad, в которой была смоделирована задача пространственного распределения поля звуковой волны от N-источников информации и N-акустических систем компенсации поля волны. Анализируя полученные результаты, можно сделать вывод о возможности создания акустической системы адаптивного подавления информационного сигнала, но для определенных условий. Для всех рассмотренных частот в центре распределения мощности компенсации излучений наблюдается область с достаточно низким уровнем излучения, окруженная более высокими амплитудными составляющими, что дает возможность использования этой зоны для ведения, например, защищенных переговоров. Такая система может оказаться наиболее эффективной и простой в технической реализации по защите информации при условии создания сферической волны как от источника информации (человека), так и компенсирующей акустической системы.

Что же касается создания системы защиты от утечки по акустическому каналу при распространении плоских затухающих и плоских незатухающих волн, то сделан вывод, что для данной ситуации, когда есть 2 источника информационного сигнала и 2 акустические подавляющие системы, реализация защиты невозможна. В этом случае следует предположить, что для защиты необходимо использовать большее количество акустических систем с определенной амплитудой, расположенных на определенном расстоянии.

ACOUSTIC SYSTEM OF ADAPTIVE SUPPRESSION OF INFORMATIVE SIGNAL

RostislavСазонов,BorisЖуриленко
NATIONAL AVIATION UNIVERSITY

Systems of adaptive suppression of acoustical signal it is possible to make an effort apply for defence of acoustic information in an apartment. Thus within the limits of guard zone by means of the compensative acoustic systems an area, outside that sound-level either is absent, relaxes either considerably, is created or distorted to the illegible state. Therefore there is of interest research of spatial distribution of the field of sound-wave from information and acoustic systems of indemnification of the field of wave generators.

For the achievement of the put aim the электронно-вычислительная environment of Mathcad, in that the task of spatial distribution of the field of sound-wave was modelled from N- of information and N- of the acoustic systems of indemnification of the field of wave generators, was used. Analysing the got results, it is possible to draw conclusion about possibility of creation of the acoustic system of adaptive suppression of informative signal, but for certain terms. For all considered frequencies in the center of distribution of power of indemnification of radiations there is an area with the low enough level of radiation, surrounded by higher peak constituents, that gives an opportunity of the use of this zone for a conduct, for example, of the protected negotiations. Such system can appear most effective and simple in technical realization on a priv on condition of creation of spherical wave both from an information(man) generator and compensative acoustic system. As for creation of the system of protecting from a loss on an acoustic channel at distribution of flat discontinuous and flat undamped waves, then drawn conclusion, that for this situation, when 2 sources of informative signal and 2 acoustic repressing systems are, realization of defence is impossible. In this case it is necessary to suppose that for defence it is necessary to use the greater amount of the acoustic systems with certain amplitude, located on certain distance.

УДК 004.056.5:534.87(045)

ДИФЕРЕНЦІАЛЬНИЙ ПІДСИЛЮВАЧ ДЛЯ ВИЯВЛЕННЯ АКУСТОЕЛЕКТРИЧНИХ ПЕРЕТВОРЮВАЧІВ

Євген Дубовий
Національний Авіаційний Університет

Стаття: ***5 стор., 7 джерел.***

Людська мова є природним і найпоширенішим способом обміну інформацією між людьми і може викликати механічні коливання елементів електронної апаратури, що в свою чергу, призводить до появи в ній паразитних напруги електричних струмів і електромагнітних випромінювань .

Оцінюючи можливості захисту конфіденційних переговорів у приміщенні, доцільно передбачити можливість використання зловмисником елементів апаратури для перехоплення конфіденційної інформації, що мають в собі акустоелектричний ефект – ланцюги дзвінків телефонних апаратів, вторинний годинник, динаміки мереж трансляції, деякі сповіщувачі систем охоронної і пожежної сигналізації і тому подібне.

В основному витік інформативних акустичних сигналів здійснюється через допоміжні технічні засоби і системи. Допоміжні технічні засоби і системи, що знаходяться в зоні дії небезпечних акустичних сигналів, не рідко є причиною витоку конфіденційної інформації за межі контрольованої зони. Сигнали в ланцюгах допоміжних технічних систем і засобів, обумовлені дією зовнішніх акустичних полів, можуть бути вельми значними і перевищувати гранично допустимі для цих ланцюгів значення.

Отримані за результатами проведених досліджень рівні сигналу з акустоелектричних перетворювачів (таких як реле, динамік та дзвінковий ланцюг телефонного апарату) достатні для оцінки можливості витоку інформації по електричному каналу. Розроблено підсилювач, що може використовуватись як компактна заміна диференціального підсилювача «Піранья». Пристрій має коефіцієнт підсилення. достатній для проведення досліджень і значно зменшує рівень шумів.

ДИФФЕРЕНЦИОНАЛЬНЫЙ УСИЛИТЕЛЬ ДЛЯ ВЫЯВЛЕНИЯ АКУСТОЭЛЕКТРИЧЕСКИХ ПРЕОБРАЗОВАТЕЛЕЙ

Евгений Дубовый
Национальный авиационный университет

Человеческий язык является естественным и самым распространенным способом обмена информацией между людьми и может вызывать механические колебания элементов электронной аппаратуры, что в свою очередь, приводит к появлению в ней паразитных напряжения электрических токов и электромагнитных излучений. Оценивая возможности защиты конфиденциальных переговоров в помещении, целесообразно предусмотреть возможность использования злоумышленником элементов аппаратуры для перехвата конфиденциальной информации, которые имеют в себе акустоелектричний эффект - цепи звонков телефонных аппаратов, вторичные часы, динамика сетей трансляции, некоторые извещатели систем охранительной и пожарной сигнализации, и тому подобное.

В основном утечка информативных акустических сигналов осуществляется через вспомогательные технические средства и системы. Вспомогательные технические средства и системы, которые находятся в зоне действия опасных акустических сигналов, не редко являются причиной утечки конфиденциальной информации за пределы контролируемой зоны. Сигналы в цепях вспомогательных технических систем и средств, обусловленные действием внешних акустических полей, могут быть весьма значительными и превышать предельно допустимые для этих цепей значения.

Полученные по результатам проведенных исследований уровни сигнала из акустоелектричних преобразователей (таких как реле, динамик и цепь колокола телефонного аппарата) достаточные для оценки возможности утечки информации по электрическому каналу. Разработан усилитель, который может использоваться в качестве компактной замены дифференциального усилителя «Пиранья». Устройство имеет коэффициент усиления, достаточный для проведения исследований и значительно уменьшает уровень шумов.

THE DIFFERENTIAL STRENGTHENER FOR EXPOSURE OF ACOUSTOELECTRIC TRANSFORMERS

Yevhen Dubovoj
National Aviation University

A human language is the natural and the most widespread method of exchange information between people and can cause the mechanical vibrations of elements of electronic equipment, which in turns to the appearance in it of stray voltage electrical currents and electromagnetic radiation. Assessing the ability to protect confidential conversations in the room, it is expedient to provide for the possibility of using elements of the apparatus by an attacker to intercept confidential information, which have an acoustoelectric effect - a chain of calls telephones, the secondary clock, speaker broadcast networks, some protective systems, detectors and fire alarms, etc. .

Most leaks informative acoustic signals through assistive technology and systems. Assistive technology and systems that are in range of dangerous acoustic signals are not uncommon cause of leakage of confidential information outside the controlled area. The signals in the circuits of assistive technology systems and facilities, due to the influence of external acoustic fields can be significant and exceed the maximum allowable values for these chains.

Obtained from the results of studies of the signal levels acoustoelectric converters (such as relays, speaker and circuit telephone bell) are sufficient to assess the possibility of information leakage on the electrical channel. Developed amplifier that can be used as a compact replacement of the differential amplifier "Piranha." The device has a gain, sufficient for research and greatly reduces the noise level.