Security of Wireless Sensor Network with Random Access Control

UDC 004.7: 62-519: 621.391

[1] Oleksandr Korchenko,
[2] Mikolaj Karpinski, [2] Stanislaw Rajba
[1] *National Aviation University, Ukraine, icaocentre@nau.edu.ua,*
[2] *University of Bielsko-Biala, Poland, mkarpinski@ath.bielsko.pl, stanislaw.rajba@gmail.com*

Wireless sensor networks (WSN) create a new quality in modern systems, acquisition and transfer of information. We propose the concept of WSN with random moments of time-signal emissions with a one-way transmission using one radio frequency. We use Poisson Arrivals See Time Average (PASTA) for modeling probability of a collision during the transmission of the radio network to control the correct network operation. Implementation of WSN puts an entirely new requirements for the radio communication and control processes, which manage to meet the increasingly sophisticated technologies. The use of radio communications in the network-type convergecast is much more difficult than in a well-operated radio broadcasting systems and conciliation point-to-point. The main difficulty lies in the organization of radio traffic which is represented by the controlled access to the transmission medium which in other terms represents the surrounding space. In the surrounding area, an active space in the radio communication is defined by the value of the electric field which produces a transmitting device at a given point of space. There can be only one sender at a particular frequency. The WSN conditions limiting the power supply and energy supply sources capacity constitute the primary problem of determining the solutions further consequences. For this reason, frequent solution is the multi-hop topology, than the single-hop requires more energy for the radio transmission. The multi-hop network requires more complex communication algorithms. Low level of radiated power, can be an advantage on the one hand, but on the other hand it also creates communication problems. It is assumed that the various communication no that can move in a field study of the physical effects are controlled by the sensors. Thus, the mobility of nodes is assumed, which often entails changes in WSN configuration, and in particular, changes in the conditions required for the propagation of electromagnetic waves.

The sensors are completely independent from each other and their on or off state is of no influence on the operation of WSN. All the sensor- senders or a part of them may be mobile provided that their senders have been left within the radio range of the receiving base. Collision excludes the possibility of the correct receiving of information by the receiving base. Such a disturbed signal is ignored. We must accept a certain loss of information in exchange for simplicity in respect of both system and equipment. Communication protocols and reduced energy consumption of nodes have a significant impact on the improving of WSN reliability, as well as significantly increase the security of the information transmitted on WSN. The proposed model WSN access allows the improvement of the reliability and security of information.

Аналіз міжнародних стандартів управління інформаційною безпекою серії ISO 27k

УДК 004.056(043.2)

[1] Сергій Гнатюк, [2] Андрій Труфанов, [3] Олексій Тіхоміров, [4] Рустем Умєров, [1] Кирило Ануфрієнко
[1] Національний авіаційний університет, Україна, {s.gnatyuk, akp}@nau.edu.ua, [2] Іркутський державний технічний університет, Російська Федерація, troufan@istu.edu, [3] Проектний центр ООН з питань державного управління, Республіка Корея, tikhomirov@hotmail.com, [4] Громадська організація «Терра Таврида», АР Крим, Україна, rustem.amdy.umerov@gmail.com,

Головним завданням стандартів інформаційної безпеки є узгодженість позицій та запитів виробників, споживачів і аналітиків класифікаторів продуктів інформаційних технологій (ІТ). Кожна з категорій фахівців оцінює стандарти та вимоги і критерії, які в них існують, за своїми особистими параметрами. Для споживачів найбільшу роль відіграє простота критеріїв та однозначність параметрів вибору захищеної системи, а для найбільш кваліфікованої частини споживачів – гнучкість вимог та можливість їх застосування до специфічних ІТ-продуктів та середовища експлуатації. Виробники продуктів та послуг, в свою чергу, потребують від стандартів максимальної конкретності та спільних вимог і критеріїв з сучасними прогресивними технологіями. Фахівцям у галузі інформаційної безпеки сьогодні майже неможливо обійтися без знань відповідних стандартів і специфікацій. На це є декілька причин. Формальна причина полягає у тому, що необхідність дотримання певних стандартів закріплена законодавчо. Також, є більш переконливі причини: по-перше, стандарти і специфікації – одна з форм накопичення знань (насамперед на процедурному і програмно-технічному рівнях інформаційної безпеки). У них зафіксовані апробовані, високоякісні рішення та методології, розроблені найбільш кваліфікованими фахівцями; по-друге, і ті, і інші є основним засобом забезпечення взаємної сумісності апаратно-програмних систем та їх компонентів. З точки зору України, можна виділити міжнародні та державні стандарти у галузі інформаційної безпеки. Крім того, у банківській галузі (яка беззаперечно є найрозвинутішою, з точки зору інформаційної безпеки, у нашій державі) прийняті відповідні галузеві стандарти. Серед міжнародних стандартів варто виділити серію ISO 27k, що присвячена побудові системи управління інформаційною безпекою (СУІБ). Аналіз чинних стандартів зазначеної серії і є основною метою цієї роботи.

Серія ISO 27k на сьогодні включає у себе такі міжнародні стандарти:

ISO/IEC 27000:2012 Information technology — Security techniques — Information security management systems — Overview and vocabulary. Цей стандарт містить огляд та словник термінів, що відносяться до СУІБ. Огляд стандартів серії ISO27k показує яким чином необхідно використовувати ці стандарти для планування, впровадження, сертифікації та експлуатації СУІБ. Словник (глосарій) містить ретельно сформульовані формальні дефініції більшості базових термінів, пов'язаних з інформаційною безпекою, що використовуються у стандартах ISO27k.

ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements. Стандарт містить вимоги у галузі інформаційної безпеки щодо створення, розвитку і підтримки СУІБ. У ньому описані кращі світові практики в галузі управління інформаційною безпекою. ISO 27001 встановлює вимоги до СУІБ для демонстрації здатності організації захищати свої інформаційні ресурси. Основою стандарту є система управління ризиками, пов'язаними з інформацією (така система дозволяє визначити на якому конкретно напрямі інформаційної безпеки потрібно зосередити увагу та скільки часу і коштів можна витратити на певне технічне рішення для захисту інформації).

ISO/IEC 27002:2013 Information technology — Security techniques — Code of practice for information security controls. До 2007 р. цей стандарт називався ISO/IEC 17799 (опублікований у 2000 р., фактично копія Британського стандарту BS 7799-1:1999). Стандарт ISO 27002 висвітлює найкращі практичні поради щодо менеджменту інформаційної безпеки для тих, хто відповідає за створення, реалізацію або обслуговування СУІБ.

ISO/IEC 27003:2010 Information technology — Security techniques — Information security management system implementation guidance. У цьому стандарті розглядаються найважливіші аспекти, необхідні для успішної розробки та впровадження СУІБ відповідно до стандарту ISO 27001. У ньому описується процес визначення і розробки СУІБ від запуску до складання планів впровадження, також описується процес отримання схвалення керівництвом впровадження СУІБ, визначається проект впровадження СУІБ. Крім того, представлені рекомендації щодо планування проекту СУІБ, у результаті якого виходить кінцевий план впровадження СУІБ.

ISO/IEC 27004:2009 Information technology — Security techniques — Information security management — Measurement. Стандарт містить рекомендації щодо розробки та використання вимірювань і мір вимірювання для проведення оцінки ефективності реалізованої СУІБ, а також заходи і засоби контролю та управління відповідно до ISO 27001.

ISO/IEC 27005:2011 Information technology — Security techniques — Information security risk management. Цей стандарт забезпечує рекомендації щодо менеджменту ризиків інформаційної безпеки в організації відповідно до стандарту ISO 27001. Однак, цей стандарт не визначає конкретної методології для менеджменту ризиків інформаційної безпеки. Він призначений для визначення в організації підходу до менеджменту ризиків в залежності, наприклад, від галузі діяльності СУІБ, галузі застосування менеджменту ризиків або певного сектору промисловості.

ISO/IEC 27006:2011 Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems. Стандарт ISO 17021 встановлює критерії для органів, що здійснюють аудит і сертифікацію систем управління організацій. Якщо ці органи повинні бути акредитовані, як відповідні стандарту ISO 17021, з метою проведення аудиту та сертифікації СУІБ відповідно до ISO 27001, то необхідні

додаткові вимоги та керівництва до ISO 17021. Вони представлені саме у цьому стандарті.

ISO/IEC 27007:2011 Information technology — Security techniques — Guidelines for information security management systems auditing. Цей стандарт є керівництвом щодо управління програмами аудиту СУІБ та проведення внутрішніх і зовнішніх аудитів відповідно до вимог стандарту ISO 27001.

ISO/IEC TR 27008:2011 Information technology — Security techniques — Guidelines for auditors on information security management systems controls. Цей стандарт є керівництвом для всіх аудиторів СУІБ. Він підтримує процес управління ризиками інформаційної безпеки, а також внутрішні, зовнішні та сторонні аудити СУІБ, пояснюючи зв'язок між СУІБ елементів управління, що її підтримують. Крім того, цей стандарт підтримує організації, що використовують ISO 27001 та ISO 27002 у якості стратегічної платформи для управління інформаційною безпекою.

ISO/IEC 27010:2012 Information technology — Security techniques — Information security management for inter-sector and inter-organisational communications. Стандарт надає керівництво із взаємодії і зв'язку щодо інформаційної безпеки між галузями одного сектору промисловості, у різних галузях промисловості і з урядами, а також у період кризи і для захисту критичної інфраструктури чи для взаємного визнання в нормальних умовах ведення бізнесу відповідно до договірних чи інших зобов'язань.

ISO/IEC 27011:2008 Information technology — Security techniques — Information security management guidelines for telecommunications organizations based on ISO/IEC 27002. Це керівництво щодо СУІБ у галузі телекомунікації було розроблено спільно з ITU і ідентично за текстом стандарту ITU-T X.1051. Прийняття цього стандарту дозволить телекомунікаційним організаціям забезпечити базові вимоги щодо управління інформаційною безпекою (конфіденційність, цілісність, доступність).

ISO/IEC 27013:2012 — Information technology — Security techniques — Guidance on the integrated implementation of ISO/IEC 27001 & ISO/IEC 20000-1. Цей стандарт є керівництвом щодо впровадження інтегрованих інформаційної безпеки та управління IT-послугами, на основі як ISO 27001 і ISO 20000-1 (управління IT-послугами специфікації, отримані з ITIL) – дві системи управління, які доповнюють і підтримують одна одну.

ISO/IEC 27014:2013 — Information technology — Security techniques — Governance of information security. Цей стандарт є керівництвом щодо створення концепції і принципів управління інформаційною безпекою, за допомогою яких організації (різних типів і розмірів) можуть оцінити, корегувати, контролювати діяльність організації щодо інформаційної безпеки.

ISO/IEC TR 27015:2012 — Information technology — Security techniques — Information security management guidelines for financial services. Стандарт забезпечує керівництво щодо впровадження інформаційної безпеки та управління нею відповідно до ISO 27002. Він зорієнтований на розробку, реалізацію, підтримку і покращення інформаційної безпеки в організаціях, що надають фінансові послуги.

ISO/IEC TR 27019:2013 — Information technology — Security techniques — Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry. Стандарт надає керівні принципи на базі ISO 27002 для управління інформаційною безпекою систем управління технологічними процесами, які використовуються у галузі енергетики. Метою цього стандарту розширення стандартів серії ISO 27000 щодо систем управління технологічними процесами, які використовуються у галузі енергетики, і можливість створення відповідних СУІБ.

ISO/IEC 27031:2011 Information technology — Security techniques — Guidelines for information and communications technology readiness for business continuity. Цей стандарт містить концепції та принципів щодо застосування інформаційно-комунікаційних технологій для забезпечення безперервності бізнесу. Стандарт пропонує структури та фреймворки (набори методів і процесів) для будь-якох організацій – приватних, урядових і неурядових. Визначає критерії та оцінки готовності інформаційно-комунікаційних технологій організацій забезпечити безперервність бізнесу.

ISO/IEC 27032:2012 Information technology — Security techniques — Guidelines for cybersecurity. Цей стандарт є керівництвом щодо підвищення рівня кібербезпеки у контексті її унікальності та неперетину з іншими доменами безпеки, а саме: з інформаційною безпекою, безпекою приватних мереж, Інтернет-безпекою, безпекою застосунків та захистом критичної інформаційної інфраструктури. У стандарті проводиться огляд базових відомостей (включаючи термінологію) щодо кібербезпеки, наводиться співвідношення кібербезпеки з іншими зазначеними доменами безпеки та загальні принципи інформаційної взаємодії у процесі вирішення актуальних проблем кібербезпеки.

ISO/IEC 27033-1:2009 Information technology — Security techniques — Network security — Part 1: Overview and concepts. Стандарт містить огляд мережевої безпеки і пов’язаних з нею понять. Визначаються та описуються концепції, пов’язані з мережевою безпекою, а також надаються рекомендації щодо управління безпекою мережі. Мережева безпека у цьому стандарті визначається як безпека обладнання, безпека управління діяльністю, пов’язаною з пристроями, застосунками / послугами та кінцевими користувачами, як додаток до безпеки інформації, що передається каналами зв’язку.

ISO/IEC 27033-2:2012. Information technology — Security techniques — Network security — Part 2: Guidelines for the design and implementation of network security. У цьому стандарті даються практичні рекомендації щодо організації процесів планування, проектування, впровадження та документування мережевої безпеки на підприємствах. Також, наводяться критерії щодо вибору мережевого обладнання певних вендорів і шаблони документів для опису безпеки різних компонентів мережевої архітектури.

ISO/IEC 27033-3:2010 Information technology — Security techniques — Network security — Part 3: Reference networking scenarios — Threats, design techniques and control issues. Цей стандарт описує загрози, методи

проектування і питання управління відповідно до різних мережевих сценаріїв. Для кожного сценарію стандарт забезпечує детальне керівництво щодо протидії загрозам безпеці, безпеки конструкції і питання управління, які є необхідними для усунення пов'язаних ризиків. У деяких випадках у стандарті наводяться посилання на ISO 27033-4 та ISO 27033-6 (які поки є лише драфтами) для уникнення дублювання змісту цих документів. У цілому, цей стандарт спрямований на реалізацію мережевої безпеки у будь-яких організаціях.

ISO/IEC 27033-5:2013 Information technology — Security techniques — Network security — Part 5: Securing communications across networks using Virtual Private Networks (VPNs). Стандарт дає керівні принципи відбору, реалізації та моніторингу технічного контролю, що необхідно для забезпечення мережевої безпеки за допомогою технології VPN (забезпечення захищених з'єднань усередині мережі та безпечні підключення віддалених користувачів).

ISO/IEC 27034-1:2011 Information technology — Security techniques — Application security — Part 1: Overview and concepts. Стандарт забезпечує керівництво для допомоги організаціям щодо інтеграції засобів захисту в процесах, що використовуються для управління своїми застосунками. Зокрема, він містить визначення понять, принципи і процеси щодо розробки різного роду застосунків та забезпечення їх захисту.

ISO/IEC 27035:2011 Information technology — Security techniques — Information security incident management. Цей стандарт замінив свого попередника ISO 18044, що був чинним з 2004 р. Він встановлює рекомендації щодо менеджменту інцидентів інформаційної безпеки і стосується керівників підрозділів з інформаційної безпеки, інформаційних систем, сервісів та мереж. У стандарті ISO 27035 висвітлено структурний підхід до: виявлення, звітування та оцінки інцидентів інформаційної безпеки; реагування та керування інцидентами інформаційної безпеки; виявлення, оцінювання та управління уразливостями інформаційної безпеки; постійного поліпшення стану інформаційної безпеки та процесу управління інцидентами у результаті управління інцидентами та уразливостями.

ISO/IEC 27037:2012 Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence. Стандарт містить рекомендації для конкретних видів діяльності щодо роботи з цифровими доказами (зокрема, виявлення, збір, придбання і збереження цифрових фактів, які можуть мати доказове значення). Він містить рекомендації для різноманітних ситуацій, що виникають у процесі цифрової оброблення даних і допомагає організаціям щодо їх дисциплінарних процедур та сприяє обміну потенційними цифровими доказами між різними юрисдикціями.

Таким чином, у цій роботі проведено аналіз чинних стандартів серії ISO 27k (включаючи ті стандарти, що біли прийняті протягом минулого року), виділено їх цілі, особливості, а також взаємозв'язки. Отримані результати є систематизованими знаннями і будуть корисними для ефективної розробки та впровадження СУІБ у державних та комерційних структурах.

Іноземний досвід побудови інформаційного суспільства

УДК 35.746.1
Олена Солодка
Національна академія Служби безпеки України, Україна, sweet27@ukr.net

Аналіз міжнародного досвіду показує, що не існує єдиної успішної програми розвитку інформаційного суспільства. Кожна стратегічна програма чи план мають бути індивідуальними й враховувати специфічні особливості окремо взятої країни або регіону, підходи до розвитку інформаційного суспільства відрізняються навіть у розвинутих країнах. Так, у США увага акцентується на технологічних аспектах, у Європі – на соціальних вимірах.

Пріоритетом політики США є розвиток інформаційної інфраструктури. Відомою ініціативою, яка реалізується у США з 1993 р., є "Національна інформаційна інфраструктура: план дій", згідно з якою визнається, що інформаційну інфраструктуру створює переважно приватний сектор, при цьому держава повинна відігравати істотну роль для забезпечення усіх інформаційними ресурсами за доступними цінами.

Європейська модель інформаційного суспільства відрізняється стратегією європейської інтеграції, пошуками рівноваги між контролем держави і ринком, динамічним поєднанням державних інтересів і приватного бізнесу. Характерними рисами європейської моделі виступають варіативність програм побудови інформаційного суспільства для різних країн, зумовлених новою європейською геополітикою, становленням інформаційної економіки**.**

Сучасні інформаційні і телекомунікаційні технології значною мірою обумовлюють ті зміни, які відбуваються на сьогодні в суспільстві і державі.

Зокрема, відбувається суттєва активізація використання інформаційно-комунікаційних технологій в органах державної влади, що сприяє розширенню сфери надання послуг за допомогою інформаційно-комунікаційних технологій, створення інформаційних масивів даних (статистика, законодавство, Інтернет-сайти державних органів), підвищення ефективності діяльності самих державних органів, а також їх відкритості, разом з цим виникає питання побудови ефективної системи протидії кібератакам.

У процесі становлення інформаційного суспільства держава відіграє роль координатора діяльності різних суб'єктів суспільства, який за допомогою цілеспрямованої політики сприяє інтеграції людей до нового інформаційно-технологічного середовища, розвитку галузей інформаційної індустрії, формуванню інформаційного права, зміцненню демократії і забезпеченню прав людини.

Разом з цим, на порядок денний виносяться проблеми захисту інформації, яка перебуває в обігу у зазначених мережах, зокрема персональних даних, а також порядок їх вилучення у разі необхідності чи бажання власника, т.зв. права особи “бути забутою”, що на сьогодні надзвичайно актуалізується у ЄС з огляду на те, що на інформаційна мережа є глобальною і неможливо встановити її кордони.

"Критичні" теми в інформаційному просторі як індикатор загроз національній безпеці України

УДК 004.912

Валентина Панченко
Національна академія СБ України, Україна, inf_sec@ukr.net

Дане дослідження ґрунтується на припущенні, що інформаційний простір (множина інформаційних повідомлень інформаційних агентств, ЗМІ, інтернет-видань, офіційних сайтів державних установ, інтернет-ресурсів політичних, громадських та ін. організацій) є проекцією подій реального світу. Окрім відомостей про події реального світу, інформаційний простір містить повідомлення, спрямовані на маніпулювання суспільною свідомістю (Г. Шиллер, 1980).

У 2006 році під час дослідження інформаційного відображення подій щодо блокування "місцевим населенням" у Феодосії спільних військових навчань Україна-НАТО «Сі Бриз-2006» нами було сформовано перелік тем, які використовувались у вітчизняному інформаційному просторі з метою маніпулювання суспільною свідомістю: федералізм (сепаратизм), статус Криму, Чорноморський флот РФ, міжконфесійна ворожнеча, міжнаціональна ворожнеча, расизм, статус російської мови, масові протести, військово–політичне співробітництво України з НАТО, інтеграція в ЄС, утиски демократії, протистояння гілок влади, неефективність правоохоронних органів, торгівля зброєю, енергозалежність України, фінансово–економічна криза, соціальна справедливість, меншовартість України (В. Панченко, В. Полевий, 2007). Такі теми ми назвали "критичними", оскільки вони викликають резонанс, є предметом постійних дискусій та конфліктів в українському суспільстві. Виявилось, що на фоні "феодосійського конфлікту" в інформаційному просторі були збурені теми федералізму (сепаратизму), статусу Криму, підстав для перебування Чорноморського флоту РФ на території Криму, статусу російської мови. Разом з тим, тема неефективності правоохоронних органів мала від'ємну кореляцію (- 0,67) з темою "феодосійського конфлікту". Тобто, на той час проблема масових протестів у зв'язку із проведенням спільних навчань не пов'язувалась із проблемою неефективності правоохоронних органів України. За результатами дослідження було доведено, що з боку РФ проводилася спеціальна інформаційна операція, стратегічною метою якої був подальший розкол України за мовно-етнічною ознакою.

Метою даного дослідження є вивчення динаміки часових рядів, які характеризують зазначені вище "критичні" теми в умовах дій РФ щодо анексії Криму. У доповіді представлені результати порівняльного аналізу часових рядів, які характеризують ці теми у 2006 році під час "феодосійського конфлікту" та у 2014 році в умовах дій РФ щодо анексії Криму. Результати дослідження, а також останні події в Україні переконливо свідчать, що "критичні" теми, які циркулюють в інформаційному просторі, є індикатором загроз національній безпеці.

Принципи дезінформування як інформаційної технології впливу

УДК 35.078.3:025.4.03
Володимир Шлапаченко
Національна академія Служби безпеки України, Україна, shlap65@yandex.ua

В умовах інформаційного суспільства дезінформацію (дезінформування) слід розглядати як ефективну та фінансово доступну технологію інформаційно-психологічного впливу на особу (групу осіб), уповноважену приймати рішення (ОУПР), засобом якої є спеціально модифікована інформація, з метою формування у неї (них) хибної уяви про певні події, факти, явища, та, завдяки цьому, спонукання її (їх) до прийняття певних рішень (вчинення певних дій або бездіяльності), вигідних суб'єкту впливу (тобто, фактично маніпулювання нею).

Найпоширенішою та найвідомішою сферою застосування дезінформування ще донедавна була військово-політична сфера. Своєчасне та переконливе введення в оману противника надавало значну тактичну перевагу, а за певних умов – забезпечувало і стратегічну перемогу. З перетворенням інформації, по суті, в стратегічний ресурс, застосування дезінформування, як технології, що здатна забезпечити реалізацію інтересів суб'єктів її просування чи не у всіх сферах суспільного життя, набуло популярності та поширення. В той же час, попри те, що «центр тяжіння» дезінформування поступово зміщується у сферу економіки, науки та соціально-політичних процесів, аналіз проведення спеціальних інформаційних операцій (СІО) в сучасних локальних воєнних конфліктах свідчить про те, що застосування дезінформування у військово-політичній сфері і досі залишається найбільш поширеним, чи не найефективнішим та найкраще теоретично розробленим. Особливу роль в поширенні дезінформації на сьогодні відіграють ЗМІ (друковані та електронні видання, телебачення, радіомовлення, мережа Інтернет) Посилення світової конкурентної боротьби держав в умовах інформаційного суспільства перетворило сучасні ЗМІ на потужний інструмент досягнення переваг в політичній, економічній, воєнній, соціальній, духовній та інших сферах діяльності суспільства, що за ефективністю застосування не поступається воєнним діям, економічним санкціями, політичній ізоляції тощо.

Виходячи з того, що для громадян глобалізованого світу ЗМІ стали не лише домінуючим, але й часто, - єдиним джерелом отримання інформації, проведення заходів дезінформування з залученням ЗМІ, за таких умов, відкриває сприятливі можливості щодо збільшення не лише масштабів та тривалості впливу, але й його потужності та глибини сприйняття, оскільки дозволяє використовувати нові мультимедійні, маніпуляційні та психологічні техніки. Подовжена тривалість такого впливу послаблює аналітичні фільтри свідомості, сприяє зростанню маніпуляційної уразливості людини, зокрема й ОУПР та, зрештою, полегшує досягання мети дезінформування.

Кінцевою метою (запланованим результатом) дезінформування є досягнення певних переваг в результаті сприятливої поведінки (дії чи бездіяльності) об'єкта інформаційно-психологічного впливу.

Основними принципами дезінформування визначаємо наступні:

*Чітка спрямованість***.** Розробник дезінформації має чітко уявляти кого і з якою метою він має ввести в оману, яка прогнозована поведінка якого об'єкта

дезінформації є кінцевою метою запланованих заходів. З огляду на це розвідувальні служби противника, як правило, не є самостійним об'єктом стратегічної дезінформації, а являють собою лише канал для передачі необхідної (модифікованої) інформації ОУПР, оскільки саме вона є кінцевою метою впливу для досягнення мети дезінформування;

Своєчасність. Дезінформування, як спеціальна інформаційна операція, вимагає ретельного розрахунку часу. Має бути передбачено час на виконання всіх її етапів.

Правдоподібність інформації, що просувається. Досягається особливістю її модифікації, з урахуванням уявлень та конкретних знань об'єкта у цій сфері, має корелювати з його внутрішніми переконаннями та забезпечувати можливість підтвердження при перевірці з інших джерел. Передбачає використання значної частини правдивої інформації (як відомої так і не відомої ОУПР, яка має надати достовірності всьому масиву інформації, що просувається, а також певну креативність у способах доведення дезінформації. Полягає у досягненні вірогідного сприйняття дезінформації об'єктом.

Узгодженість комплексних заходів з дезінформування з загальною концепцією просування дезінформації та її метою.

Секретність планування та проведення передбачає:

- уникнення витоку інформації про цілі дезінформації, факт проведення заходів дезінформування, зміст модифікованої інформації, заходи її впровадження, тощо;

- диференційована обізнаність виконавців щодо плану проведення заходів (лише в частині, що стосується);

- завчасне розроблення легенди прикриття та відповідних заходів «димової завіси» в разі часткової розшифровки заходів з дезінформування.

Доцільність. Вигода (політична, економічна воєнна тощо) від проведення дезінформаційної СІО має переважати ризики (економічні, політичні, воєнні тощо) в разі часткової розшифровки, зриву чи провалу операції.

Критерієм ефективності проведення дезінформаційних заходів є оцінка того, наскільки і в якій мірі вдалося вплинути на об'єкта дезінформації, спонукати його до прогнозованих дій (у визначених суб'єктом рамках) щодо прийняття відповідного рішення на підставі доведених дезінформаційних матеріалів.

Втім, небезпечність дезінформувння полягає не лише в можливості отримання якоїсь конкретної переваги, на яку вона, власне, і була спрямована, а ще й в тому, що навіть одна успішна СІО з дезінформування має продовжуваний дезорієнтаційний вплив, оскільки негативно впливає на здатність об'єкта об'єктивно оцінювати інші (наступні) здобуті відомості (щодо спецслужб – розвідувальні), ставлячи під сумнів їх достовірність. А це, у свою чергу, відкриває нові можливості застосування дезінформування «від зворотнього».

В сучасному інформаційному суспільстві дезінформування, як явище, постійно змінюючись, продовжує удосконалюватися. Використовуються усе більш витончені методи поширення спотвореної інформації. Усе це вимагає подальших ґрунтовних досліджень форм і методів дезінформування, удосконалення заходів протидії дезінформаційним СІО, насамперед в галузі нормативно-правового регулювання інформаційної діяльності та забезпечення інформаційної безпеки.

Автоматизація обробки неструктурованих текстів для потреб аналітики

УДК 004.912

Денис Савченко
Національна академія Служби безпеки України, Україна, sdensys@gmail.com

Невідповідність між темпами зростання обсягів неструктурованої текстової інформації в сучасних комп‘ютерних мережах і наявними людськими ресурсами для її опрацювання формує проблему інтелектуалізації методів обробки такої інформації в автоматизованих інформаційних системах.

За різними оцінками, від 80% до 90% інформації, яка на сьогодні зберігається в комп‘ютерних системах і мережах, представлена у неструктурованому або слабоструктурованому вигляді. При цьому, лише приблизно десята частина з цього об‘єму може бути використана в класичних системах автоматизованої обробки структурованої інформації та аналітики.

Не дивлячись на те, що інтерес до роботи з неструктурованими даними з‘явився у світі ще з 50-х років XX століття, розвиток методів їх обробки відбувався не з такою швидкістю, з якою зростали їх об‘єми, і така ситуація зберігалась аж до початку нового тисячоліття.

Виділення обробки неструктурованих даних (Unstructured Data Analysis) в якості окремої науково-технічної задачі датовано початком 2000 років, коли аналітики Меріл Лінч (Merrill Lynch) і Гартнер (Gartner) оприлюднили інформацію про неочікувано значні втрати часу при роботі з даними, пов‘язані з відсутністю автоматизації опрацювання контенту. На той час на середніх підприємствах прямі збитки в результаті цього у перерахуванні на одного працівника складали за оцінками від 2,5 до 3,5 тисяч доларів США на рік.

Утім, подібні сигнали аналітиків не сприймались всерйоз аж до останніх часів, коли з 2008-2009 років набули значного поширення нові джерела неструктурованих даних: соціальні мережі, мобільні пристрої, реєстраційна апаратура, які протягом декількох років сформували проблему «великих даних» (Big Datas). Як наслідок, невідповідність великих об‘ємів інформації застарілим методам її обробки значно підвищила інтерес наукових кіл до зазначеної проблематики.

Основою сучасних систем автоматизованої обробки неструктурованої текстової інформації є так звана «комп‘ютерна система, заснована на смислі» (Meaning-Based Computing), а їх суть зводиться до демонстрації часткових рішень з галузі, яку можна віднести до «керування знаннями» (Knowledge Management).

Складовими елементами таких систем є технології автоматизованого пошуку інформації за певними критеріями в інформаційних масивах (Information Retrieval), технології витягування з неструктурованої інформації окремих компонентів і зберігання їх як метаінформації (Information Extraction), а також технології глибинного аналізу текстів (Text Mining). При цьому, відповідно до методології, що склалася, до основних елементів останньої відносяться реферування (summarization), виявлення феноменів (feature extraction), класифікація (classification), кластеризація (clustering), відповідь на питання (question answering), тематичне індексування (thematic indexing),

створення онтологій (ontology engineering), засоби підтримки і створення таксономії (taxonomies) і тезаурусів (thesauri) тощо.

Загалом всі існуючі сучасні підходи щодо автоматизованої обробки неструктурованих текстів можна умовно поділити на два класи: 1) швидкі алгоритми, які не залежать від мови і предметної області і використовують статистичні методи; 2) достатньо розвинені підходи, що дають непогані результати, але порівняно значно повільніші, які залежать від мови, предметної області і, як правило, використовують лінгвістичні методи.

Існує думка, що найбільш ефективним буде підхід, який поєднує швидкість і незалежність від мови алгоритмів першого класу з високою якістю обробки другого класу.

На сьогодні особливо актуальними є змістовні напрями розвитку аналізу неструктурованої інформації, серед яких, зокрема, можливості суміщення аналізу неструктурованої інформації з математичними методами аналізу даних. Враховуючи, що нестійкість більшості класичних алгоритмів виявляється при наявності у текстах орфографічних помилок і синонімічних замін, однією з базових задач інтелектуального аналізу неструктурованих текстів є створення механізмів, здатних ефективно працювати в умовах невизначеності проміжних результатів, стійких до навмисних і випадкових помилок у текстових одиницях, що аналізуються.

Створити подібні механізми можливо, якщо застосувати метод однозначного ототожнення будь-якої текстової одиниці, тобто заданої послідовності символів певного алфавіту, з відповідним числом або групою чисел. При цьому, зазначений метод повинен характеризуватися деякими суттєвими властивостями.

По-перше, він повинен характеризуватися низькою вірогідністю колізій, тобто низькою вірогідністю існування двох або більше різних текстових одиниць, яким відповідає одне й те ж саме число або група чисел. Враховуючи, що подібна властивість притаманна хеш-функціям, такий метод, як передбачається, буде різновидом хеш-функції. В такому випадку число або група чисел, яке відповідає певній текстовій одиниці, буде її хешем.

По-друге, цей метод повинен характеризуватися прямою залежністю різниці між двома будь-якими текстовими одиницями (в контексті сприйняття цієї різниці людиною) від математичної різниці хешів цих текстових одиниць, тобто мова йде про перцептивність такого методу.

В різні часи у вітчизняній та іноземній науці проблемами міри текстових одиниць і відстанями між текстами займались такі дослідники як Ж. Селтон, В. Левенштейн, Д. Гасфілд, Ф. Дамерау, Ф. Дженсен-Шеннон, Р. Хеммінг, однак комплексного дослідження саме методу перцептивного хешу тексту на сьогодні не існує. В той же час застосування методу перцептивного хешу наразі обмежується лише завданнями обробки графічної інформації.

Практична значущість подібного дослідження полягає в можливості побудови за його результатами програмних систем автоматизованого моніторингу та обробки неструктурованої текстової інформації в комп‘ютерних мережах на основі більш ефективних методик і механізмів.

Організаційні заходи безпекового супроводу реалізації національних інтересів в умовах глобалізації

УДК 681.3+519.83
Володимир Богданович, Олександр Довгань
Національна академія СБ України, Україна, bogdnr11@gmail.com, Державний університет телекомунікацій, dod16.67@mail.ru

Очевидним є той факт, що захист національних інтересів повинен мати комплексний характер і базуватися на глибокому аналізі можливих негативних наслідків. Система забезпечення національної безпеки має бути здатною ефективно реагувати на загрози в різних сферах. До того ж у системі повинні економно витрачатися ресурси, які виділяються на забезпечення національної безпеки. Теоретично можна будувати захист з орієнтацією на всі можливі загрози, але це економічно недоцільно. Безумовно, не можна забезпечити безпеку держави і суспільства, не захистивши їх від імовірного збройного нападу, економічної блокади, політичного диктату або зовнішнього інформаційно-психологічного пресингу. Здатність протистояти зовнішній дії формується усередині країни. Тому не можна не бачити взаємозумовленість внутрішніх і зовнішніх викликів. По-перше, можливості держави із попередження й запобігання зовнішнім загрозам багато в чому визначаються її здатністю вирішувати свої внутрішні проблеми. Виключно важливе, якщо не вирішальне значення в організації діяльності із забезпечення державної безпеки має суб'єктивна сторона сприйняття загроз. Попри об'єктивну природу загроз безпеці, віддзеркалення людиною цього явища часто не відповідає реальному становищу. Оцінка об'єктивно наявної загрози завжди несе в собі елементи суб'єктивізму і вже через це є спотвореним відображенням об'єктивної дійсності. Інколи спотворення в сприйнятті загрози можуть досягати значних масштабів. Більше того, загроза реально існує, формується, а суб'єкти безпеки можуть не знати про це, не усвідомлювати катастрофи, що насувається (наприклад, надмірне захоплення уряду кредитами іноземних банків перетворює країну на вічного боржника зі всіма наслідками). По-друге, і вихід із внутрішніх труднощів, і попередження, і нейтралізація зовнішніх загроз багато в чому полегшує, а то й повністю забезпечує підтримка світової спільноти, особливо стратегічних партнерів. По-третє, у взаємопов'язаному світі, повному глобальних проблем, безпека будь-якої країни не може бути повністю гарантована без усунення регіональних і міжнародних небезпек. Натомість дестабілізація обстановки в одній країні, її внутрішні конфлікти інтернаціоналізуються, що посилює зв'язок внутрішніх і зовнішніх проблем безпеки. Скажімо, стверджується, що в нинішніх умовах на безпеку України найбільший вплив мають внутрішні чинники (відсутність єдності влади, соціально-політична нестабільність, корупція, зниження якості й рівня життя людей, зростання злочинності тощо). Але багато цих небезпек підтримується зовнішніми силами. Тому стратегія безпеки, з одного боку, повинна мати комплексний характер, будуватися не як спосіб протидії окремим загрозам, а становити комплексний підхід, що враховує багатогранність властивостей і різноманітність інтересів України, усі зв'язки й можливі наслідки.

Сопровождение подвижных объектов для банковской структуры

УДК 004.056(043.2)
Гульнур Жангисина, Отрнер Евгений
Казахский национальный технический университет им. К.И. Сатпаева, Казахстан, gul_zhd@mail.ru

Проведенный анализ существующих систем и комплексов технических и программных средств сопровождения подвижных объектов показал, что технические средства бортовых устройств и каналообразующая аппаратура используемых средств связи в существующих системах, малопригодна для решения всего спектра задач, стоящих перед организациями и ведомствами, а анализ методов определения местоположения подвижных объектов позволяет сделать однозначный выбор в пользу метода радионавигации.

Аппаратно-программные средства существующих ССПО, как правило, позволяют эффективно решать только одну задачу, а именно передачу информации о местоположении подвижного объекта в центр управления.

Вместе с тем, рассматриваемые мною ведомства, требует передавать и другую важную производственную информацию: разработка и контроль соблюдения маршрутов и графиков движения; контроль состояния перевозимого груза и физического состояния водителя; обеспечение обмена формализованными сообщениями между ДЦ и ТС; обеспечение оперативного реагирования аварийными службами и службами автотранспортных предприятий в случае возникновения критических ситуаций; автоматизированное формирование и коллективное использование соответствующих банков данных всеми структурами обеспечения безопасности перевозочного процесса.

Таким образом, возникает альтернатива: первое - дополнительно к существующим в этих ведомствах информационно-телекоммуникационным средствам добавить полностью автономные аппаратно-программные средства передачи навигационных данных о подвижных объектах и каким-то образом интегрировать их в единую информационно-телекоммуникационную среду организации; второе - на базе единой существующей аппаратно-программной платформе сбора и обработки информации обеспечить обмен навигационными и производственными данными между подвижными объектами и ДЦ.

Проведенный анализ указывает на целесообразность применения второго подхода, так как, с подвижных объектов необходимо передавать не только информацию о маршруте его движения и текущем местоположении, но и производственные данные, обработка которых должна осуществляться средствами единой информационной системы, функционирующей в конкретной организации или ведомстве. Кроме того, не потребуется установка дублирующих средств передачи и обработки данных. Более того, выделяется отдельное направление развития и расширения функциональных возможностей существующей информационно-телекоммуникационной системы организации.

На этапе разработки технологии контроля местоположения и маршрутов подвижных объектов на основе спутниковой системы мониторинга объектов

мною было принято решение о том, что информационный обмен между ДЦ и множеством подвижных объектов необходимо осуществлять существующими в системе «ГЛОНАСС-Банк» средствами приема/передачи информации не прибегая к интеграции аппаратных и программных средств сторонних производителей.

В настоящее время в крупных инкассационных службах в городах Республики Казахстан существует огромное количество проблем, таких как: координация деятельности различных служб; управление и контроль работы техники; управление движением транспортных потоков; повышение качества транспортного обслуживания населения; вопросы безопасности.

Для решения вышеперечисленных проблем, предлагается Система Мониторинга Безопасности и Управления подвижными объектами ГЛОНАСС-Банк. Такая система позволит обеспечить централизованный контроль и управление подвижными объектами предприятия.

Система мониторинга мобильных объектов позволяет:

-Определять местоположение объектов и отображать их на электронной карте;

-Определять и отображать параметры движения объектов: скорость, направление движения, пройденный маршрут, места и продолжительность остановок;

-Контролировать состояние датчиков, установленных на мобильном объекте;

-Удаленно управлять исполнительными устройствами, установленными на мобильном объекте;

-Контролировать маршрут движения;

-Получать своевременное оповещение о входе или выходе из заданных географических зон;

-Пользоваться встроенными стандартными отчетами;

-Формировать отчёты по различным показателям за любой период времени;

-Формировать архивы о перемещении объектов и происшедших с ними событиях.

Используя систему Глонасс-Банк, можно: увеличить объём перевозок и количество предоставляемых услуг; снизить аварийность; продлить срок эксплуатации транспортных средств; повысить дисциплину персонала; исключить нецелевое использование транспорта; оптимизировать расход топлива и ГСМ; защита и обмен формализованными сообщениями между ДЦ и ТС.

Предлагаемая система включает в себя специальные аппаратно-программные решения, позволяющие осуществлять контроль и оперативное управление специальными службами, непрерывный мониторинг транспорта предприятий и организаций, обеспечить персональную безопасность.

Дослідження ефективності використання експертної системи технічної діагностики з традиційною структурою

УДК 004.82

Анна Коваленко, Олексій Смірнов
Кіровоградський національний технічний університет, Україна,
anna__sun@mail.ru, assa_s@mail.ru

Дослідження останніх тенденцій розвитку інформаційних технологій при побудові систем навігації та спостереження в рамках державної науково-технічної програми створення державної інтегрованої інформаційної системи, а також ряду робіт показують гостру необхідність створення підсистеми технічної діагностики інтегрованої інформаційної системи (далі ІІС).

Через велику кількість об'єктів діагностики, складності та некоректності протоколів різних рівнів завдання технічної діагностики ІІС погано формулюється. А значить, традиційні способи технічної діагностики (апаратний і функціональний контроль) будуть малоефективними.

Найбільш перспективним підходом до вирішення цього завдання є розробка і створення експертної системи (далі ЕС) технічної діагностики ІІС.

Така система повинна отримувати дані від ІІС та оцінювати поточний стан мережі та її об'єкти, здійснювати пошук несправностей, прогнозувати подальший розвиток ситуації на об'єктах діагностики, представляти отримані результати в зручній для розуміння оператором формі. Аналіз тенденцій розвитку ІІС показує, що розвиток йде по шляху ускладнення об'єктів мережі, протоколів їх функціонування з метою підвищення ефективності та надійності мережі. Що призводить до підвищення надійності роботи, і ускладнення пошуку несправностей через ідентичність симптомів.

Мета дослідження визначити ефективність використання традиційних ЕС для вирішення завдань технічної діагностики ІІС. ЕС являє собою комплекс програм і апаратних засобів, які імітують деякі процеси розумової діяльності фахівця при вирішенні кола завдань.

Проведені дослідження показали, що ЕС з традиційною структурою не підходить для діагностики ІІС. Це викликано наступними причинами: функціонування системи здійснюється тільки на основі знань, отриманих від експерта; моделі подання знань орієнтовані на прості і добре структуровані області; існує велика кількість не виражених явно відомостей, прихованих в структурах представлення знань. Це обумовлено тим, що не всі пропозиції експерта знайшли відображення в моделі предметної області, включеної в систему; реалізація механізму виведення тільки за умови повноти і несуперечності знань і даних; поповнення знань і перевірка їх на несуперечність здійснюється людиною; розбіжність структури знань про предметну область в ЕС і у експерта.

Всі наведені недоліки свідчать про неефективність використання традиційних ЕС для вирішення завдань технічної діагностики ІІС. Необхідна розробка такої структури ЕС, яка враховувала б зазначені вище недоліки ЕС з традиційною архітектурою, а також особливостей технічної діагностики ІІС.

Дослідження впливу кількості ланок стохастичних генераторів на покращення їх статистичних характеристик

УДК 004.421.5

[1,2] Марія Мандрона, [2] Володимир Максимович
[1]*Львівський державний університет безпеки життєдіяльності, Україна,*
[2]*Національний університет «Львівська політехніка», Україна,*
mandrona27@gmail.com, volodymyr.maksymovych@gmail.com

Розвиток засобів захисту інформації, обчислювальної і вимірювальної техніки, а також із впровадженням новітніх технологій значно розширює сферу застосування генераторів псевдовипадкових послідовностей (ГПВП).

Серед відомих технологій криптографічного захисту інформації особливе місце займають методи формування псевдовипадкових послідовностей. Вони використовуються практично в усіх механізмах криптографічного захисту інформації і призначені для вироблення послідовностей чисел, які володіють певними статистичними властивостями.

Перспективним напрямком є використання стохастичних алгоритмів для захисту комп'ютерних систем від випадкових і навмисних деструктивних впливів. З використанням стохастичних генераторів вирішуються такі завдання, як забезпечення секретності і конфіденційності інформації, підтвердження автентичності суб'єктів інформаційної взаємодії, контроль процесу виконання програм, забезпечення цілісності об'єктів (повідомлень, масивів даних) інформаційної взаємодії. Стохастичними є всі протоколи захищеного взаємодії віддалених абонентів.

Практично всі алгоритми генерації псевдовипадкових послідовностей мають певні вади, зазвичай це – занадто короткий період вихідної послідовності, наявність кореляції між різними її членами, нерівномірний розподіл, передбачуваність, недостатня швидкість і т.д. Основною проблемою при проектуванні ГПВП є важке розв'язання протиріччя між якістю сформованих псевдовипадкових послідовностей та ефективністю програмної та апаратної реалізації. Тому актуальним науковим та інженерним завданням є розробка нових генераторів, які поєднують у собі високу швидкодію і хороші статистичні властивості сформованої псевдовипадкової послідовності .

Метою роботи є дослідження статистичних характеристик багатоланкових генераторів псевдовипадкових послідовностей з використанням R-блоків при різних варіантах побудови.

У роботі, з допомогою імітаційних моделей, досліджуються 3 варіанти ГПВП з використанням R-блоку (ГПВП_1-ГПВП_3). Псевдовипадкова бітова послідовність формувалась на виході молодшого розряду одного з регістрів генераторів.

На рис. 1 наведено схему одноланкового генератора (ГПВП_1), який складається з 4 регістрів і одного R-блока.

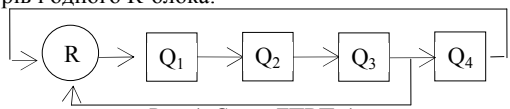

Рис. 1. Схема ГПВП_1

Рівняння, що описує роботу R-блоку має вигляд

$$R_H = H((m_{Q_3} + Q_4) mod\, 2^n). \quad (1)$$

ГПВП_2 є дволанковим генератором зі збільшеною кількістю регістрів генераторів – 4 і 6, вихідні послідовності яких додаються за модулем два. Рівняння, що описують роботу R-блоків мають вигляд

$$R1_H = H((m_{Q_{13}} + Q_{14}) mod\, 2^n), \quad (2)$$

$$R2_H = H((m_{Q_{24}} + Q_{26}) mod\, 2^n). \quad (3)$$

У рівняннях (4-6) описується робота R-блоків триланкового генератора (ГПВП_3), який складається з трьох генераторів по 4, 5 і 6 регістрів, виходи яких додаються за модулем два.

$$R1_H = H((m_{Q_{11}} + Q_{13}) mod\, 2^n), \quad (4)$$

$$R2_H = H((m_{Q_{22}} + Q_{25}) mod\, 2^n), \quad (5)$$

$$R3_H = H((m_{Q_{35}} + Q_{31}) mod\, 2^n). \quad (6)$$

Оцінювання статистичних характеристик досліджуваних генераторів здійснювалось за допомогою набору тестів NIST STS. Результати тестування наведені у табл. 1. При тестуванні розрядність регістрів генератора змінювалась.

Таблиця 1. Результати тестування ГПВП_1- ГПВП_3

Статистичний тест NIST STS	ГПВП_1					ГПВП_2					ГПВП_3				
	Розрядність генератора, n														
	12	*10*	*9*	*8*	*4*	*12*	*10*	*9*	*8*	*4*	*12*	*10*	*9*	*8*	*4*
Частотний тест	+	+	+	+	-	+	+	+	+	+	+	+	+	+	+
Частотний блоковий тест	+	+	+	-	-	+	+	+	+	+	+	+	+	+	+
Тест накопичених сум	+	+	+	+	-	+	+	+	+	-	+	+	+	+	+
Тест на серійність	+	+	+	+	-	+	+	+	+	-	+	+	+	+	+
Тест найдовшої серії з одиниць	+	+	+	+	-	+	+	+	+	-	+	+	+	+	+
Тест рангу бінарних матриць	+	+	+	-	-	+	+	+	+	+	+	+	+	+	+
Тест на основі дискретного перетворення Фур'є	+	+	+	+	-	+	+	+	+	+	+	+	+	+	+
Тест шаблонів без перекриття	+	+	+	+	-	+	+	+	-	-	+	+	+	+	+
Тест шаблонів з перекриттям	+	+	+	+	-	+	+	+	+	-	+	+	+	+	+
Універсальний статистичний тест	+	+	+	+	-	+	+	+	+	+	+	+	+	+	+
Тест на основі апроксимованої ентропії	+	+	+	+	-	+	+	+	+	-	+	+	+	+	+
Тест випадкових блукань	+	+	+	+	-	+	+	+	+	-	+	+	+	+	+
Тест випадкових блукань 2	+	+	+	+	-	+	+	+	+	-	+	+	+	+	+
Тест серій	+	+	+	+	-	+	+	+	+	-	+	+	+	+	+
Тест лінійної складності	+	+	+	+	-	+	+	+	+	+	+	+	+	+	+

Із результатів тестування можна зробити висновок, що статистичні характеристики стохастичних генераторів псевдовипадкових послідовностей побудованих з використанням R-блоків покращуються із збільшенням кількості ланок, задіяних регістрів і кількості їх двійкових розрядів. Авторами розроблено схему генератора, статистичні характеристики яких проходять весь набір тестів NIST STS з позитивними результатами, навіть при розрядності регістрів 4 біт.

Моделювання та дослідження DDOS-атак

УДК 004.056

Віталій Марченко
Інститут кібернетики ім. В.М. Глушкова НАН України, Україна,
vmarchenko@gmail.com

Останнім часом DDOS-атаки стали одним з основних інструментів проведення конкурентної боротьби та ключовим елементом кіберзброї. Тому питання дослідження методів організації та проведення різноманітних класів розподілених атак на відмову в обслуговуванні є актуальною та важливою в контексті розвитку інформаційного суспільства та розбудови електронних представництв державних органів.

Одною з базових проблем вивчення та дослідження сучасних методів реалізації DDOS-атак є складність їх моделювання в реальних середовищах з використанням повнофункціональних інформаційних систем, в якості цілей для атаки та створення і реалізація відповідних векторів атак. Для вирішення вказаної проблеми було розроблено ряд моделюючих комплексів, для дослідження методів та алгоритмів проведення DDOS-атак. Одним з таких комплексів є OMNET++ з відповідними фреймворками INET та NETA. Він дозволяє досить ефективно проводити моделювання різноманітних векторів DDOS-атак використовуючи гетерогенні моделі комп'ютерних мереж. При цьому гетерогенність мереж розуміється як одночасне використання провідних мереж з різною архітектурою та безпровідних мереж, а також нових типів мереж таких як Ad-hoc, Mash і т.п.

Останні досягання в області створення сучасних апаратних засобів дозволили реалізувати досить потужні мобільні пристрої(телефони, планшети і т.п.) які можуть самі виступати в якості агентів нападу. А це в свою чергу кардинальне змінює не тільки особливості їх організації, а й самі умови проведення атак. Зокрема при дослідженні DDOS-атак потрібно враховувати гетерогенний характер комп'ютерних мереж, в яких знаходяться агенти нападу, на відміну від раніше розповсюдженого підходу, де в якості агентів виступав стандартизований ПК з постійним під'єднанням до мережі. Використання мобільних терміналів, в якості агентів нападу, робить малоефективними існуючі методи виявляння DDOS-атак. Так як одним з основних методів ідентифікації активної фази атаки є аналіз і виявлення шаблонів аномального мережевого трафіку. Використання великої кількості мобільних агентів нападу або учасників різноманітних p2p-мереж значно ускладнює подібну задачу. Тому що в основі подібних методів виявлення лежить деяка статичність розташування джерел трафіку для ідентифікації аномальності відповідних значень. В гетерогенних мережах присутня непередбачуваність розташування джерел трафіку та постійна його зміна. При цьому навіть успішне виявлення джерел не дозволяє з достатньою ефективністю провести блокування відповідної активності, так як будуть заблоковані мережі в яких знаходяться джерела, а не самі агенти.

Таким чином дослідження DDOS-атак в гетерогенних мережах є актуальною задачею для створення ефективних засобів захисту.

Оцінка інформаційних загроз процесу функціонування віртуальних спільнот

УДК 004.738

[1]Андрій Пелещишин, [2] Руслан Гумінський
[1] Національний університет "Львівська Політехніка", Україна, e-mail – apele@ridne.net, [2] Науковий центр Сухопутних військ Академії сухопутних військ, Україна, e-mail – gruslan@meta.ua

Аналіз інформаційних потоків великого обсягу інформації в інтернет середовищі, їх адаптивного агрегування та узагальнення ускладнюються відсутністю типових методик і рішень, неповнотою відповідних технологічних підходів. В дослідженнях вітчизняних та зарубіжних науковців показником інформаційної загрози використовується кількісна динаміка яка характеризується, як кількість подій за одиницю часу або кількість повідомлень, що мають відношення до їх інформаційного наповнення. Дане визначення інформаційної загрози підходить для аналізу інформаційних інтернет ресурсів, як оцінка інтенсивності публікацій за відповідною тематикою.

В той же час, при аналізі інформаційних загроз в віртуальних спільнотах, які утворюються за допомогою соціальних мереж, необхідно враховувати не тільки їх інформаційне наповнення, а також і кількість учасників віртуальної спільноти та структуру зв'язків між елементами (дискусіями) в спільноті.

Для оцінки інформаційних загроз авторами сформований показник інформаційної загрози процесу функціонування віртуальної спільноти, як кількісна оцінка реалізації інформаційної загрози, яка несе інформаційне наповнення дискусій віртуальної спільноти.

При формуванні показника інформаційної загрози автори врахували наступні складові: кількість учасників віртуальної спільноти, кількість можливого мобілізаційного ресурсу, якість інформаційного наповнення віртуальної спільноти та структуру зв'язків дискусій у віртуальній спільноті.

Для визначення показника інформаційної загрози процесу функціонування віртуальної спільноти автори використали цінність віртуальної спільноти, яка враховує кількість учасників та зв'язки між ними, використовуючи закон помірного зростання цінності мережі. Цінність віртуальної спільноти - це потенційна доступність учасників спільноти, з якими любий учасник спільноти може «зв'язатися» в разі необхідності.

Таким чином, показник інформаційної загрози процесу функціонування віртуальної спільноти в загальному має вигляд:

$$InfTreat(VirtualCommunity) = \begin{cases} \dfrac{Value(VirtualCommunity)}{Value(VirtualCommunity)^*}, \\ 1, якщо \dfrac{Value(VirtualCommunity)}{Value(VirtualCommunity)^*} > 1 \end{cases},$$

де $Value(VirtualCommunity)$ - цінність віртуальної спільноти; $Value(VirtualCommunity)^*$ - критична цінність віртуальної спільноти, при якій

реалізується інформаційна загроза без урахування якості інформаційного наповнення віртуальної спільноти, структури зв'язків дискусій у віртуальній спільноті. Використовуючи закон помірного зростання цінності мережі, визначимо цінність віртуальної спільноти з урахуванням кількості її учасників:

$$Value(VirtualCommunity) = \sum_{i=1}^{M} ThreadMembers_i \cdot \ln\left(\sum_{i=1}^{M} ThreadMembers_i\right) - \\ - \sum_{i=1}^{M} ThreadMembers_i ,$$

де $ThreadMembers_i$ - кількість учасників *i*-ої дискусії; M – кількість дискусій у віртуальній спільноті.

Критична цінність віртуальної спільноти:

$$Value(VirtualCommunity)^* = Members(InfTreat_i) \cdot \ln\left(Members(InfTreat_i)\right) - \\ - Members(InfTreat_i) ,$$

де $Members(InfTreat_i)$ - критична кількість учасників віртуальної спільноти, визначеної експертами, при якій реалізується *i*-та інформаційна загроза без урахування якості інформаційного наповнення віртуальної спільноти, структури зв'язків дискусій у віртуальній спільноті.

Наступні складові (якість інформаційного наповнення віртуальної спільноти та структура зв'язків дискусій в віртуальній спільноті) будуть зменшувати цінність віртуальної спільноти.

З урахуванням всіх складових показника інформаційної загрози загальний вираз цінності віртуальної спільноти має вигляд:

$$Value(VirtualCommunity) = \sum_{i=1}^{N}\left(\sum_{j=1}^{M^{(Group_i)}}\left(Sim(Thread_j)\cdot ThreadMembers_j\right)\cdot\right.$$

$$\left.\cdot \ln\left(\sum_{j=1}^{M^{(Group_i)}}\left(Sim(Thread_j)\cdot ThreadMembers_j\right)\right) - \sum_{j=1}^{M^{(Group_i)}}\left(Sim(Thread_j)\cdot ThreadMembers_j\right)\right) + ,$$

$$+ card\left(Shadow(VirtualCommunity)\right)$$

де $ThreadMembers_j$ - кількість учасників *j*-ої дискусії; $Sim(Thread_j)$ - міра відповідності тематичного напрямку *j*-ої дискусії; $M^{(Group_i)}$ - кількість дискусій в *i*-ій групі; N – кількість груп у віртуальній спільноті, які характеризують структуру віртуальної спільноти; *Shadow(VirtualCommunity)* - множина зареєстрованих користувачів соціальних мереж, які зацікавлені ідеологією (тематикою) віртуальної спільноти та не є учасниками дискусії - можливий мобілізаційний ресурс.

Таким чином, отримуємо показник інформаційної загрози з урахуванням всіх складових та виходячи з його розрахунку, він буде приймати значення в межах [0,1], що спрощує подальше прийняття рішення щодо протидії інформаційно-психологічного впливу процесу функціонування віртуальних спільнот.

Протокол доказательства с нулевым разглашением на эллиптических кривых

УДК: 004.056.55: 003.26

Алексей Онацкий
Одесская национальная академия связи им. А.С. Попова, Украина,
onatsky@mail.ru

Применение открытых каналов передачи данных создает потенциальные возможности для действий злоумышленников (нарушителей). Поэтому одной из важных задач обеспечении информационной безопасности при взаимодействии пользователей является использование методов и средств, позволяющих одной (проверяющей) стороне убедиться в подлинности другой (проверяемой) стороны. Для этого, применяют протоколы доказательства с нулевым разглашением (zero-knowledge proof – ZKP). Широкое распространение при идентификации получили протоколы ZKP на базе ассиметричного шифрования: Fiat–Shamir, Schnorr, Okamoto, Guillou–Quisquater, Brickell–McCurley, Feige–Fiat–Shamir. Корректность и стойкость данных протоколов определяется дискретным логарифмированием в простом конечном поле Z_n/Z_p, а также увеличением количества циклов аккредитации при разных случайных значениях r и x.

С развитием методов и средств криптоанализа, а также быстрого развития технологий и мощности вычислительных компьютерных систем, возникает необходимость увеличивать размеры общесистемных параметров протокола, вследствие чего увеличивается ресурсоемкость и сложность выполнения базовых операций в полях. Однако решение данного вопроса может быть достигнуто за счет реализации протоколов ZKP на основе математического аппарата эллиптических кривых, что позволяет значительно уменьшить размер параметров протокола и увеличить криптографическую стойкость.

В работе предложен новый протокол ZKP на основе эллиптических кривых (Elliptic Curves – EC) над конечными полями.

Протокол доказательства с нулевым разглашением на основе эллиптических кривых (рис. 1). Пусть $E_p(a, b)$ – эллиптическая кривая, известная участникам информационного процесса, G и Q – предварительно согласованные и опубликованные точки этой кривой. Абонент A выбирает секретные числа k_1 и k_2 $(1 < k_1, k_2 < n)$ и вычисляет открытый ключ $Y_a = k_1G + k_2Q$, который передает абоненту B вместе с заявкой γ.

Абонент B выбирает секретное число k_b $(1 < k_b < n)$ и вычисляет открытый ключ $Y_b = k_b(G + Q)$, который передает абоненту A вместе с запросом x.

Протокол:

1. Абонент A выбирает случайные числа r_1 и r_2, $1 < r_1, r_2 < n - 1$ и отправляет абоненту B заявку γ: $A \rightarrow B$: Y_a, $\gamma = r_1G + r_2Q$;
2. Абонент B отвечает случайным запросом x: $A \leftarrow B$: Y_b, x;
3. Абонент A отправляет абоненту B значения y_1, y_2, y_3:

$A \rightarrow B$: $y_1 = (r_1 + xk_1)Y_b$, $y_2 = (r_2 + xk_2)Y_b$, $y_3 = (r_1 + xk_1)Q + (r_2 + xk_2)G$.

Абонент B проверяет равенство $k_b^{-1}(y_1 + y_2) - y_3 - xY_a = \gamma$.

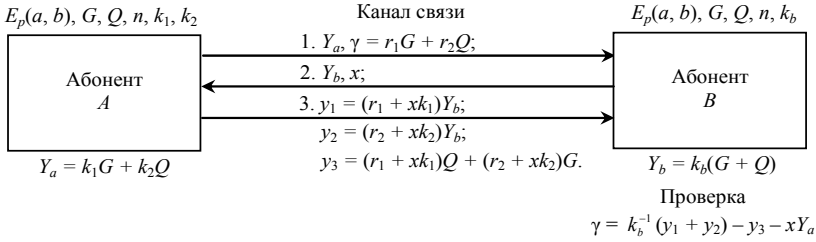

Рис. 1. Протокол ZKP на основе эллиптических кривых

Полнота. Доказывающий A знает значения k_1 и k_2, поэтому он в состоянии ответить на любой запрос x абонента B. При этом проверяющий B убеждается в справедливости соотношения

$$(y_1 + y_2)\, k_b^{-1} - y_3 - xY_a = (r_1 + xk_1)\, Y_b\, k_b^{-1} + (r_2 + xk_2)\, Y_b\, k_b^{-1} -$$
$$- (r_1 + xk_1)Q - (r_2 + xk_2)G - x(k_1G + k_2Q) = r_1G + r_2Q = \gamma.$$

Для анализа предложенного протокола ZKP EC на устойчивость к атакам противника был применен программный продукт AVISPA. Выбор данного продукта обусловлен тем, что AVISPA интегрирует все современные подходы к анализу протоколов, такие как проверка на модели, древовидные автоматы, временная логика. Главное преимущество AVISPA, в отличие от других средств (REVERE, Athena, NRL Protocol Analyzer, FDR, HERMES, ProVerif) состоит в том, что ее применение позволяет не только определить, есть ли недостатки у конкретного протокола, но и найти атаки на данный протокол.

Проверка модели предложенного протокола была выполнена с помощью Protocol Simulation пакета SPAN. Программная верификация протокола и устойчивость протокола к атакам противника была выполнена с помощью программных модулей OFMC и CLAtSe. В результате проверки протокола ZKP EC известных атак на протокол не найдено.

Выводы. Криптографические протоколы, основанные на доказательстве с нулевым разглашением, позволяют произвести процедуры идентификации, обмена ключами и другие криптографические операции без утечки секретной информации в течение информационного обмена. В работе предложен новый криптографический протокол ZKP EC. Определена полнота и корректность протокола, приведены примеры расчета, выполнена проверка модели и верификация протокола. Для проверки протокола ZKP EC на устойчивость к атакам противника были применены средства пакета SPAN для AVISPA. В результате проверки протокола известных атак на протоколы не найдено. Противник может получить доступ к информации, только решив задачу дискретного логарифмирования в группе точек эллиптической кривой. Следовательно, при использовании протокола ZKP EC, позволяет значительно уменьшить размеры параметров протокола и увеличить криптографическую стойкость.

Дослідження ризиків інсайдерських атак

УДК 004.056

Вадим Савчук
Національний технічний університет України «КПІ», Україна,
vadima.savchuk@gmail.com

Інформаційна безпека, як відомо, має справу з двома категоріями загроз: зовнішніми і внутрішніми. На сьогоднішній день реалізовано достатньо багато засобів для боротьби з зовнішніми загрозами, але іще недостатня наукова база для дослідження внутрішніх порушників. Актуальність даної тематики полягає в тому, що чим більших успіхів досягає людство в боротьбі з зовнішніми кіберзагрозами, тим рішучіше на перший план виходять загрози внутрішні, з якими за статистикою пов'язано більше 70% відсотків усіх інцидентів безпеки.

Сутність даної проблеми проявляється при проектуванні інформаційних систем на підприємствах та організаціях, і полягає в тому, що найбільш поширені канали витоку відносяться до категорії ненавмисного розкриття з причин необізнаності або недисциплінованості.

Ймовірність вдалої реалізації загрози P_t це:

$$P_T = P_t P_v , \qquad (1)$$

де P_v – ймовірність вдалого використання зловмисником вразливостей інформаційної системи (ІС), а P_t це ймовірність активації (виникнення) загрози. В загальному випадку P_v – узагальнена (інтегрована) ймовірність успішного проведення комплексу атак, породжених існуванням сукупності вразливостей ІС (включно із вразливостями самої системи захисту інформації (СЗІ)). Тобто значення ймовірності P_v залежить від ступеню захищеності ІС, який в свою чергу зумовлюється обсягом інвестувань в СЗІ (величиною c), і певним чином враховується співвідношенням

$$P_v = \frac{q}{q + sc} , \qquad (2)$$

де s – коефіцієнт, можливий діапазон значень якого пов’язаний з існуючою у світовій практиці залежністю між рівнем інвестицій c у СЗІ та цінністю критичної інформації для її власника.

Формула (2) застосовна для обчислення P_v у випадку «ображеного інсайдера» або «нелояльного інсайдера», тоді як у разі «впроваджених» або інсайдерів «що підробляють» (наведені терміни як і формули (1)-(3) запозичено із статті Архипова О.Є., Скиби А.В, "Інформаційні ризики: методи та способи дослідження, моделі ризиків і методи їх ідентифікації", ж. Захист інформації №4, 2014) оцінювання ймовірності реалізації вразливостей виконується за виразом:

$$P_v = \frac{q}{q + s\frac{c^2}{D}} \qquad (3)$$

Крім то, можливо побудувати оптимізаційну схему, за якою можна буде зробити висновки щодо ефективності та доцільності інвестицій у СЗІ організації. Якщо D прямує до нуля то знаменник функції прямує до нескінченності, і відповідно ймовірність P_v прямує до нуля. Тобто при

мінімальних витратах порушника ймовірність вдалого використання зловмисником вразливостей інформаційної системи(P_v) наближається до нуля, що відповідає реальній ситуації. А Якщо D прямує до безкінечності то знаменник наближається до q, а значення P_v прямує до одиниці, що показує те, що зловмисник при наявності необмежених ресурсів майже напевно реалізує атаку.

Залишковий ризик в цьому випадку дорівнюватиме $R=P_tP_vq$. Таким чином величина втрат, які вдалося попередити завдяки інвестуванню в СЗІ, становить

$$R_1-R=P_tq-P_tP_vq=(1-P_v)P_tq=P_sP_tq\ , \qquad (4)$$

Крім того, чистий прибуток атакуючої сторони:

$$\Delta_R=P_vg-D=\frac{q}{q+s\frac{c^2}{D}}g-D \qquad (5)$$

Проаналізуємо співвідношення (5) як функції змінної D та дослідимо його на екстремум:

$$\frac{d\Delta_R}{dD}=\frac{c^2sgq-q^2D^2-s^2c^4}{(Dq+sc^2)^2}=0\ ,$$

$$D=-\frac{c^2s}{q}\pm c\sqrt{\frac{sg}{q}} \qquad (6)$$

Так як $D\geq 0$ отримуємо:

$$-\frac{c^2s}{q}\pm c\sqrt{\frac{sg}{q}}\geq 0\ ,$$

$$g\geq\frac{c^2s}{q} \qquad (7)$$

Якщо припустити, що виграш порушника рівнозначний втратам власника інформації, при її розголошенні, то з (7) отримуємо $c\leq q/\sqrt{s}$. Тобто при інвестиціях $c\leq q/\sqrt{s}$ порушник буде отримувати прибуток при мінімальних власних затратах. Отже обсяг інвестицій, який буде забезпечувати найменше значення Δ_R, а отже і зменшувати бажання зловмисника здійснювати протиправні дії:

$$c_{eff}=\frac{q}{\sqrt{s}} \qquad (8)$$

Значення ймовірності P_v і ризику R для цього обсягу інвестицій:

$$P_v(c_{eff})=\frac{1}{1+\frac{q}{D}}\ ,$$

$$R_T(c_{eff})=P_vP_tq=\frac{q}{1+\frac{q}{D}} \qquad (9)$$

Тепер, маючи значення інвестицій c_{eff}, ми можемо вважати їх своєрідним еталоном для того, щоб адекватно інвестувати в інформаційну безпеку.

Науковий керівник — д.т.н., професор, Олександр Архипов

Використання онтології у визначенні рівня гарантій безпеки

УДК 004.056

Олександр Романченко
Національний технічний університет України «Київський політехнічний інститут», mitrand@mail.ru

В Україні основним керівним документом для проектування, побудови і експертної оцінки комплексних систем захисту інформації (КСЗІ) є НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу». У документі висуваються вимоги до фукцій захисту (послуг безпеки) та до гарантій безпеки.

Критерії гарантій включають шість основних класів вимог: вимоги архітектури комплексу засобів захисту, середовища розробки, послідовності розробки, випробування комплексу засобів захисту, середовища функціонування і експлуатаційної документації. Сім ієрархічних рівнів гарантій відбивають поступово наростаючу міру певності в тому, що реалізовані в комп'ютерній системі послуги дозволяють протистояти певним загрозам, що механізми, які їх реалізують, в свою чергу коректно реалізовані і можуть забезпечити очікуваний споживачем рівень захищеності інформації під час експлуатації комп'ютерної системи.

На сьогоднішній день відсутні формалізовані методи оцінки виконання вимог гарантій безпеки. Нормативний документ НД ТЗІ 2.7-010-09 «Методичні вказівки з оцінювання рівня гарантій коректності реалізації функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу» у деякій мірі систематизує процес перевірки виконання рівня гарантій безпеки, проте основна задача оцінювання покладається на особу, яка здійснює оцінювання, що призводить до суб'єктивності оцінки.

Збільшити рівень довіри до результату оцінювання рівня гарантій безпеки у КСЗІ можна шляхом побудови онтологічної ієрархії предметної області гарантій безпеки, що дозволить певним чином упорядкувати і формалізувати процедуру визначення рівня гарантій безпеки.

Онтологія — це система з наборів понять (концептів) і тверджень про ці поняття, на основі яких можна будувати класи, об'єкти, відношення, функції та теорії. Формальна модель онтології O має вигляд впорядкованої четвірки $O=<X,R,F,A>$, де $X=\{x_1, x_2,\ldots,x_n\}$, $i=1\ldots n$, $n=\text{Card } X$ — скінченна множина термінів предметної області, яку описує O; $R=\{r_1, r_2,\ldots,r_m\}$, $R: r_1\times r_2\times\ldots\times r_m$, $k=1\ldots m$, $m=\text{Card } R$ — скінченна множина відношень між термінами заданої предметної області; $F:X\times R$ — скінченна множина функцій інтерпретації, заданих на термінах і/або відношеннях O; A — скінчена множина аксіом. Відношення представляють тип взаємодії між концептами предметної області.. Аксіоми використовуються для моделювання тверджень завжди істинних.

Метою даної роботи є визначення базового набору складових елементів онтології предметної області гарантій безпеки, яка може бути використана для систематизації і формалізації процесу визначення рівня гарантій безпеки.

Для структурування знань предметної області використовуються три основні категорії онтологій: 1. статичну онтологію, до якої входять сутності

предметної області, їхні властивості і відношення; 2. динамічну онтологію, що визначає ситуації, які виникають у процесі рішення проблеми, і спосіб перетворення одних ситуацій в інші; 3. епістемічну онтологію, що описує знання, які керують процесом переходу від однієї ситуації до іншої.

Відповідно до НД ТЗІ 2.5-004-99 можна визначити наступні концепти високого рівня у складі онтології предметної області гарантій безпеки, що відображають основні класи вимог до комп'ютерної системи: *архітектура* – ці вимоги забезпечують реалізацію *політики безпеки; середовище розробки* - вимоги забезпечують можливість *розробника* контролювати *процес розробки* комп'ютерної системи і може *керувати її конфігурацією* у процесі розробки; *функціональні специфікації* - забезпечують розробку *розробником політики безпеки* і її моделі; *проект архітектури; детальний проект; реалізація* - вимагає від *розробника* відповідності реалізованої комп'ютерної системи *детальному проекту*; *середовище функціонування* – забезпечує отримання і використання *замовником* не модифікованої, еталонної версії комп'ютерної системи. Концептами можна визначити осіб та організації, які беруть безпосередню участь у розробці, експлуатації та оцінюванні комп'ютерної системи: *розробник, замовник і експерт*.

Для систематизації і формалізації визначення рівня гарантій онтологія може бути розширена, а вимоги, які включаються до основних класів вимог зі зростаннямм рівня гарантій повинні бути визначені як концепти. Це забезпечує деталізацію онтології. Відношення при цьому будуть мати характер наслідування. Завдяки тому, що структура критеріїв рівнів гарантій безпеки у Критеріях є сама по собі ієрархічною, побудована для них онтології буде відрізнятися високим рівнем забезпечення принципу обґрунтованості. Таким чином можливо побудувати окрему онтологію для кожного основного класу вимог, а завдяки принципу розширення об'єднати отримані шість онтологій у одну загальну онтологію для визначення рівня гарантій безпеки.

При використанні онтології слід враховувати, що рівень гарантій безпеки визначається по мінімальному рівню виконання основних класів вимог.

Наукова новизна роботи полягає в тому, що для формалізації і забезпечення строгості оцінювання рівня гарантій безпеки пропонується використовувати онтологічний метод аналізу. В існуючих роботах подібної тематики будуються онтології предметної області самого процесу оцінки рівня гарантій. Практична значущість. Рівень довіри до результатів оцінювання значно підвищується при використанні формалізованих і систематизованих методів оцінки. Використання онтології завдяки принципам ясності і обґрунтованості дозволяє це забезпечити. Принцип розширюваності дозволяє доповнювати онтологію за необхідності, при цьому її структура не порушується. У процесі побудови онтології предметної області гарантій безпеки виявилося, що рівні гарантій безпеки у Критеріях завдяки своїй ієрархічній структурі і конкретизації кожного рівня є зручними для побудови онтології їхньої предметної області і дозволяють досягти високого рівня обґрунтованості отриманої онтології.

Науковий керівник — д.т.н., професор. Олександр Архипов

Розроблення програмного забезпечення для захисту друкованих документів

УДК 004.056.56: 655.25

[1]Марія Назаркевич, [2]Оксана.Троян
[1]*Національний університет «Львівська політехніка», Україна, м. Львів, вул.Ст.Бандери 12, nazarkevich@mail.ru,* [2]*Національний університет «Львівська політехніка», Україна, м. Львів, вул.Ст.Бандери 12, troyan.oxana@gmail.com*

Постановка проблеми. Розробити програмне забезпечення для забезпечення захисту інформації друкованих документів.

Мета дослідження. Комплексне поєднання методу побудови прихованих елементів (фонових сіток, псевдорельєфних зображень, мікрографіки) та методу графічних пасток.

Актуальність дослідження. Метод побудови прихованих елементів базується на створенні графічного зображення з роздільчою здатністю більше 2400 dpi та прихованні деякої інформації, яка стає невидимою для людського зору. Метод графічних пасток використовує побудову гравюри та латентних зображень. Графічні пастки забезпечують захист від фальсифікації.

Комплексне поєднання методу побудови прихованих елементів та графічних пасток дає можливість отримати гравюри; окремі складові зображення у шарах; підтримати логічні операції додавання, інверсію і т.д. для шарів; використати маски з регульованою прозорістю; базові та унікальні штрихування для ліній, точок та растрових зображень; створити додаткові захисні зображень з приховуванням інформації.

Наукова новизна. В перше розроблено програмне забезпечення для створення захисних елементів у вигляді графічних зображень з високою роздільчою здатністю.

Основна частина. Розроблений метод захисту призначений для створення захисних елементів. Програмне забезпечення, яке створює гравіювання на першому етапі завантажує растрове зображення, яке показане на рис. 1.

На рис. 2.1 показано фрагмент захисного зображення, де кут штрихування вибирається у певній зоні і залежить від відтінків сірого. На рис. 2.2 представлено фрагмент захисного зображення, у якому штрихування залежить від градієнтного переходу, а лінії є неперервними. На рис. 2.3 представлено фрагмент захисного зображення, у якому використовується усереднене значення кольору в цій зоні.

У програмному продукті реалізовано три різні способи утворення захисту. В залежності від вибору режиму, лінія може як просто підніматися при накладанні на зображення, так і перетворюватись у деформовану з різною амплітудою коливань. Також є можливість зміни лінії на точку в місцях накладання її на зображення. Усі методи забезпечуть високу якість зображень. Запропонована методика може бути застосована також для захисту документів, що публікуються в Інтернеті.

При виготовленні поліграфічної продукції використовують гравюри, які покращують дизайн видання та дозволяють підвищити ступінь захисту документів. Це досягається шляхом нанесення дрібних елементів. За рахунок складності утворення найдрібніших елементів – ліній у гравюрі, можна

перевірити достовірність документу. При спробі підробки, гравюру неможливо відтворити за допомогою інших технологій, які використовуються при виготовленні друку.

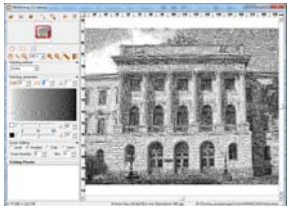

*Рис. 1. Ілюстрація роботи програми***;**

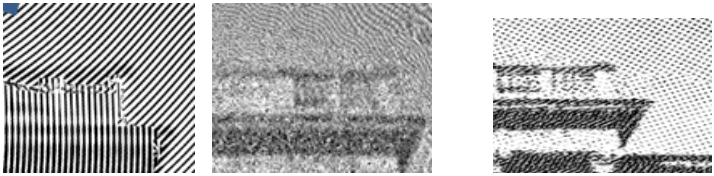

*Рис. 2. Ілюстрація роботи програми***;** *1 – згенерований рисунок методом «Рівень»***,** *2 – згенерований рисунок методом «Градієнт», 3 – згенерований рисунок методом «Колір»*

У методі побудови прихованих елементів при спробах копіюваня утворюється муар, викликаний частотою повторення цих ліній і частотою проходження відліків скануючого або друкуючого пристроїв. Муар виражається на копії помітною нерівномірності контрасту поля даних ліній щодо однорідного по інтенсивності поля оригіналу, тобто виникнення повторюваних смуг з певним періодом, відповідним різниці зазначених просторових частот. Ця нерівномірність при уважному розгляді може бути впевнено виявлена неозброєним оком або виявлена при використанні збільшувальних приладів.

У методі побудови графічних пасток використовуватися малопомітні розриви в графічних орнаментах; навмисне порушення локальної симетрії при відтворенні одного з декількох повторюваних елементів орнаменту; застосування в текстових реквізитах повторювальних знаків, що відрізняються від інших за розміром, шрифтом або нахилом і т. п.

Висновки. Розроблене програмне забезпечення формує документи з високою поліграфічною якістю. Захисні растрові зображення генеруються штрихуванням, зміною амплітуди лінії та зміною величини растрової точки.

Аналіз зловмисних програм методами нечіткої логіки

УДК 004.056

[1] Олексій Савченко
Національний технічний університет України «КПІ», Україна,
alex.usavchenko@gmail.com

На сьогоднійшній день рівень загроз, що пов'язані з кібербезпекою, значно виріс. Причиною даного явища є те, що атаки стають точковими, тобто жертви обираються не масово, і атаці передує дослідницька робота з використанням значних ресурсів: розвідки, соціальних мереж. З точки зору інформаційної безпеки, такі атаки несуть загрози конфіденційності, цілісності та доступності дипломатичній, військовій та економічній інформації держави, захист якої є критичним для країни вцілому.

Якщо ж розглянути способи реалізації даних загроз, то вони залишилися незмінними за останні декілька десятків років. Більшість зловмисних програм використовує вразливості популярного програмного забезпечення, крім того має місце психологічний фактор - довіра користувачів до виробників програмного забезпечення відомих компаній висока, і увага до їхньої безпеки низька. Таким чином, основна проблема полягає у виявленні шкідливих програм, що використовують вразливості існуючих.

Метою даної роботи є дослідження можливості використання нечіткої логіки для виявлення зловмисних програм.

Сучасні методи виявлення зловмисних програм складаються з декількох підходів. По-перше, сюди відносяться антивіруси, які в основному залежать від баз сигнатур вірусів. Антивірусна програма повинна досягати трьох цілей: сканування, виявлення, видалення. Антивірус можна визначити як функцію, що відображає програму у множину {шкідлива, не шкідлива}, тобто маємо бінарне відображення. У сучасних антивірусах, якщо запис сигнатури знайдений в базі, то програма вважається шкідливою. Таким чином, основні ризики при використанні даного підходу полягають у наступному: - використовуючи обфускацію можна обійти сканування; не шкідливі програми можуть бути розпізнані як шкідливі; з роками рівень виявлення шкідливих програм падає; неможливість виявити атаки нульового дня.

Динамічні підходи передбачають, що системні виклики представляються у вигляді математичного графу, де вершина графу - функція. Ребро графу з вершини x у вершину y означає, що виклик функції у вершині y використовує як аргумент результат, що отриманий після виклику функції у x. Таким чином представляється залежність по даним. На перший погляд, дана модель схожа на статичний аналіз, адже у обох випадках порівнюються дві структури - сигнатури та графи. Проте, досить важлива відмінність полягає в тому, що якщо статичний підхід розглядає специфічне, байтове представлення зловмисної програми, то в динамічному упор зроблений на семантику.

Велика кількість згаданих технік використовують аналіз байтових послідовностей, які можна використати для виявлення шкідливих програм. Концепція байтових послідовностей дозволяєь виявити статистичні залежності

по скомпільованому коду програми. Недоліком такого підходу є велика кількість можливих послідовностей та складність їх аналізу.

Запропонована методика передбачає використання n-грам для аналізу, але не байт коду, а послідовності API викликів програми. Для зменшення кількості досліджуваних n-грам пропонується використовувати нечіткий багатокритеріальний аналіз.

Для побудови моделі було розглянуто 7 екземплярів програм, 3 з яких вважаються не шкідливими, а 4 - шкідливими. Далі були проаналізовані уніграми API викликів даних програм з ціллю виявити залежності у кількості або послідовності викликів у зловмисних та не зловмисних програмах. Даний підхід дозволив встановити залежності по кількості уніграм. З усіх уніграм були обрані ті, що представляють інтерес з точки зору безпеки, тобто взаємодія з пам'яттю, міжпроцесова взаємодія, робота з файловою системою. Для побудови нечіткої множини були обрані 7 уніграм, представлених у табл.1.

Таблиця. 1. Обрані уніграми

GetProcAddress	U1
GetCurrentThreadId	U2
GetAsyncKeyState	U3
CommandLineToArgvW	U4
LoadLibrary	U5
CreateEventW	U6
socket	U7

Для побудови функції приналежності був використаний метод попарних порівнянь, де альтернативами виступали згадані 7 уніграм. Для них були отримані інтегральні оцінки, та побудована нечітка множина :

$$\left\{ \frac{0.64}{U7}, \frac{0.61}{U3}, \frac{0.53}{U4}, \frac{0.41}{U1}, \frac{0.39}{U2}, \frac{0.33}{U5}, \frac{0.19}{U6} \right\} \quad (1)$$

Для обраних у (1) уніграм експериментальним шляхом були встановлені порогові значення кількості уніграм, перевищення яких може означати належність програми до шкідливої.

Отримана модель була випробована на 10 зразках, рівень похибки першого роду, тобто класифікація не шкідливих програм як шкідливих складає 45%, рівень похибки другого роду, тобто класифікація шкідливих програм як не шкідливих -35%.

Отримані результати показують, що запропонована модель є досить перспективною для аналізу та виявлення зловмисних програм. З іншого боку, необхідні уточнення при виборі альтернатив. Крім того, високий рівень помилок першого та другого роду пояснюється невеликою кількістю вихідних даних.

Науковий керівник — к.ф.-м.н., доцент Микола Грайворонський

Визначення градації стану інформаційної безпеки держави

УДК 354.42
Олександр Левченко
Міністерство оборони України, avlev2009@rambler.ru

В умовах постійного посилення у світі інформаційного протиборства між державами стрімко зростає рівень та значно розширюється спектр інформаційних загроз. Реалізуючись у різних сферах життєдіяльності держави, ці загрози можуть нанести їй суттєвих втрат. Тому, для адекватного реагування на такі загрози, повинні своєчасно прийматися відповідні державницькі рішення. В основу цих рішень мають бути покладені результати оцінювання загроз інформаційній безпеці, зокрема виявлення її реального стану. Проте на сьогодні відсутні механізми визначення градації стану державної інформаційної безпеки, що негативно впливає на якість прийняття рішень.

Таким чином, метою статті є формулювання підходу до визначення градації стану інформаційної безпеки держави, що дозволить більш обґрунтовано приймати управлінські рішення.

Визначення стану інформаційної безпеки держави на відміну від відомих підходів пропонується здійснювати через визначення кількісних і якісних індикаторів, що і становить наукову новизну роботи.

За результатами порівняння наявних значень індикаторів стану інформаційної безпеки держави з їх граничними значеннями цей стан визначається як:

стабільний;

нестійкий;

вимагає прийняття невідкладних заходів.

У разі оцінки стану інформаційної безпеки як стабільного відповідними органами державної влади мають розроблятися і реалізовуватися довгострокові заходи щодо захисту національних інтересів і удосконалення системи інформаційної безпеки держави.

У разі оцінки стану інформаційної безпеки як нестійкого державним органом, що координує діяльність із забезпечення інформаційної безпеки, сумісно з виконавцями мають розроблятися і реалізуватися управлінські рішення короткострокового, середньострокового і довгострокового характеру з метою покращення стану національної безпеки в інформаційній сфері.

У разі оцінки стану інформаційної безпеки як такого, що вимагає прийняття невідкладних заходів, відповідальними органами державної влади мають формулюватися і виноситись на розгляд Кабінету міністрів України і Президенту України пропозиції щодо прийняття невідкладних заходів зі стабілізації стану інформаційної безпеки, запобігання кризових ситуацій або мінімізації їх можливих негативних наслідків.

Таким чином, застосування викладеного підходу до визначення градації стану державної інформаційної безпеки через порівняння значень кількісних і якісних індикаторів цього стану з їх граничними значеннями дозволить більш обґрунтовано приймати управлінські рішення у сфері інформаційної безпеки.

Побудова моделі оцінки мережевої безпеки з використанням динамічної Байєсової мережі

УДК 004.056(043.2)

Дмитро Мурашко
Національний технічний університет України «Київський політехнічний інститут», Україна, dmitriy_murashko@ukr.net

Змінюваний характер вразливостей в значній мірі ігнорувався в більшості існуючих робіт з метрик безпеки мережі. Основна гіпотеза полягає в тому, що загроза, що виходить від вразливості може змінюватися з плином часу в сьогоднішній динамічно змінюваній мережі. Існуючі показники безпеки, як правило, зосереджені на вимірювання індивідуальних вразливостей без урахування їх комбінованого впливу. Природа характеру розвитку вразливостей в мережах і самих мереж в значній мірі ігноруються, тому, щоб включити тимчасові чинники, такі як доступність експлойтів і патчів, слід використовувати модель на основі динамічної мережі Байєса (ДБМ).

Метою даної роботи є створення моделі, що буде враховувати різні часові аспекти вразливостей, об'єднає індивідуальні часові характеристики вразливості в глобальному рейтингу безпеки всієї мережі в будь-який момент часу. Також потрібно, щоб тимчасові тенденції та закономірності в цій моделі могли бути виявлені і використані для міркування про майбутні оцінки безпеки на основі минулих інцидентів або спостережень.

Динамічні Байесові мережі являють собою графічну модель для імовірнісних висновків у динамічних доменах, які можуть дозволити користувачам відстежувати та оновлювати систему в часі, і навіть передбачити подальші поведінку системи. У типовій моделі ДБМ, система представлена у вигляді послідовності байєсових мереж(БМ). Кожна БМ являє собою інтервал часу у ДБМ, відповідного конкретного моменту часу.

Є два входи моделі, а саме, граф атак і оцінки CVSS. Основні концепції підрахунку в CSVV є Базова оцінка (BS), Часова метрична змінна – кількісно визначає вразливість, при тому, що зміна властивостей уразливості змінюються в часі, три часові метрики, використовувані в CVSS є Вразливості (E), Рівень Відновлення (RL), і Рівень Довіри (RC).

Для зручності ми називаємо TGS = (E x RL × RC) як Часову Групову Оцінк. На підставі можливих значеннь E , RL і RC, значення TGS коливається від 0,67 до 1,0. Тимчасова оцінка (TS) визначається з BS і TGS

$$TS = round\ \_to\ \_1\ \_decimal\,(BS \times TGS)$$

Ми перетворюємо CVSS оцінки вразливості до ймовірностей шляхом перетворення оцінки BS (або TS в динамічному випадку) до ймовірності, використовуючи простий підхід поділення на розмір домену 10, та зв'язуємо цю ймовірність для всіх експлойтів, які мають цю вразливість:

$$P(e = T \mid \forall c \in R_r(e), c = T) = \frac{BS}{10}$$

Для створення моделі на основі ДБМ на прикладі графу атак G (E ∪ C, R_r ∪ R_i), представлено граф атак з використанням байєсівської мережі, яка представляє собою пару B = (G, Q), де G є орієнтованим графом, що відноситься до графу атак, введено диз'юнктивний та кон'юнктивний зв'язок виду $e_j R_i c_j$ і $c_j R_r e_{n+1}$ між експлойтами та станами, множини оцінок CSVV та широкий набір вузлів E' = E ∪ E_{BS} ∪ $E_{TGS.}$ Надалі визначаємо ДБМ як пару (B_0, B_d), де B_0 визначає попереднє P(X_1), а B_d двохзрізною часовою мережею Байєса (2TBN), яка визначає P (X_t | X_{t+1}):

$$P(X_t \mid X_{t-1}) = \prod_{t=1}^{N} P(X_t^i \mid parents(X_t^i))$$

У прикладі, значення експлойту "sunvect"(s) умовно залежить від значення експлойту вершини "addusrphp"(a). Це причинно-наслідковий зв'язок означає, що вразливість "addusrphp" повинна бути використана в першу чергу для того, щоб уразливість "sunvect" була досягнута. У цьому прикладі, головною метою є успішне використання уразливості "sunvect". Таблиці ілюструють міжзрізовий CPD. Потім ми можемо вирахувати, що P(sunvect = T) = 0,54 для першого зрізу, CPD може бути розрахована на подальші зрізи.

addusrphp		addusrphp	
T	F	T	F
$(BS_a*TGS_a)/10$	$1-(BS_a*TGS_a)/10$	0,64	0,36

sunvect			sunvect		
A	T	F	A	T	F
T	$(BS_s*TGS_s)/10$	$1-(BS_s*TGS_s)/10$	T	0,85	0,15
F	0	1	F	0	1

На сьогодення існує не так багато статей, що описують використання методологій оцінювання стандарту CSVV та інших метрик безпеки мережі. В даних статях майже відсутня обробка часових факторів в вимірюванні безпеки мережі та ігнорується природа характеру розвитку вразливостей в мережах і самих мереж. Науковою новизною роботи є запропонована модель на основі диномічної Байесової мережі, яка охоплює еволюційний характер вразливостей в комп'ютерних мережах. Показано, що ДБМ можуть бути отримані з графів атаки і стандартних значень метрики і отримана модель може бути використана для аналізу постійно змінюваних аспектів безпеки мережі. Практична значущість. Модель розроблена в тісному зв'язку зі стандартними оцінками CVSS з метою забезпечення дієвості моделі. Також модель може бути створена як для адміністраторів безпеки мережі, так і для розробників систем, що підтримують CSVV бази даних. *Науковий керівник — д.т.н. Олександр Архіпов*

Критерии эффективности методов передачи на основе энергетической, структурной и информационной скрытности

УДК 621.391
Владимир Корчинский, Денис Талакевич
Одесская национальная академия связи им. А. С. Попова, Украина,
vladkorchin@rambler.ru, denis.talakevich@gmail.com

Вхождение Украины в мировое информационное сообщество определяется успехом в решении задачи национальной программы информатизации и создании национальной сети связи Украины. Однако этот процесс сопровождается такими негативными явлениями, как компьютерные преступления и несанкционированный доступ (НСД) к секретной и конфиденциальной информации, промышленный шпионаж и прочее. Решение данной проблемы относится к задачам информационной безопасности и является важнейшей прерогативой любого государства. В стандартах ISO 7498-2, 10181-1-10181-7 предусматривается комплекс услуг безопасности с помощью различных механизмов защиты информации и, в том числе, реализуемых на основе криптографических систем на верхних уровнях эталонной модели OSI. Анализ тенденции противостояния криптографии и криптоанализа показывает, что какой бы надежной не была бы созданная криптографическая система, ее компрометация по истечении определенного срока эксплуатации очевидна. Учитывая данное обстоятельство, особый интерес приобретают методы защиты информации, которые реализуются на первом и втором уровнях эталонной модели OSI. Особенно это важно при обеспечении безопасности беспроводных сетей (например, для стандарта RadioEthernet, SM, GPRS, DPRS, CDMA и других радиосетей), так как на уровне физического канала она наиболее уязвима для перехвата передаваемых сообщений средствами НСД. Одним из путей решения этой проблемы является использование в КСС радиоэлектронной маскировки (РЭМ), которая представляет собой комплекс технических и организованных мероприятий, направленных на снижение эффективности средств радиотехнической (РР) и радиолокационной разведки. РЭМ может быть решена за счет методов передачи, обеспечивающих энергетическую, структурную, информационную и другие виды скрытности сигнальных конструкций.

Методам повышения скрытности передачи посвящено достаточно много работ, однако в литературе недостаточно уделено внимание вопросам выбора критериев эффективности скрытых методов передачи, учитывающих условия функционирования КСС (конфиденциальной системы связи) и работу систем РЭП. Поэтому, целью работы является разработка рекомендаций по выбору критериев эффективности скрытых методов передачи с учетом условий функционирования КСС.

Для оценки степени защищённости КСС от систем РЭП противника и НСД целесообразно использовать понятие помехозащищённость.

Помехозащищённость – это свойство системы не только наиболее точно воспроизводить передаваемую информацию на приемной стороне, но и способность обеспечивать её безопасность и целостность от средств РЭП и НСД с помощью реализации эффективных методов скрытности передачи.

Показатели скрытности характеризуют различные возможности системы по маскировке передаваемого сигнала по различным его параметрам.

В связи с этим различают энергетическую, структурную и информационную и другие показатели скрытности. Мерой маскировки работы КСС обосновано использовать некоторую вероятностную характеристику, которая должна учитывать основные показатели качества скрытности передачи (энергетической, структурной, информационной и др.). Такой характеристикой может быть вероятность доступности средств радиоразведки к передаваемой информации КСС:

$$P_{\delta} = P_{\acute{y}i} P_{\tilde{n}\grave{o}\delta} P_{\grave{e}i\hat{o}} \ ,$$

где P_{δ} – условная вероятность успешного решения разведкой своих задач при условии, что сигнал может быть принят, $P_{\acute{y}i}$ – условная вероятность обнаружения сеанса передачи КСС, т.е. передаваемый сигнал демаскирован за счёт решения РР проблемы энергетической скрытности; $P_{\tilde{n}\grave{o}\delta}$ – условная вероятность распознавания структуры сигнала, т.е. решена проблема защиты сигнальной конструкции за счет структурной скрытности при условии, что сигнал был перехвачен; $P_{\grave{e}i\hat{o}}$ – условная вероятность распознавания (дешифрирования) смыслового содержания перехваченного сигнала при условии, что структура сигнала была раскрыта.

Таким образом, распознавание смыслового содержания перехваченного сообщения при НСД возможно при успешных событиях обнаружения, приема и распознавании структуры сигнальной конструкции..

Общая основная проблема, которая связана с построением систем связи находится в противоречии между необходимостью, с одной стороны, передавать с предельной скоростью как можно больше информации, а, с другой стороны, обеспечить при этом высокую достоверность её приема. Для КСС не менее важным также является обеспечение энергетической скрытности передачи.

Применение сигналов с большой базой позволяет обеспечить теоретически не только любую достоверность передачи информации, но и высокую энергетическую скрытность сигнальных конструкций. Таким образом, система связи со сложными широкополосными сигналами способна работать при соотношении $P_{\tilde{n}}/P_{\o} < 1$, то есть $P_{\tilde{n}} << P_{\o}$. Это свойство обеспечивает, с одной стороны, скрытность работы передатчика конфиденциальной системы, а с другой – возможность кодового разделения каналов.

В процессе радиоэлектронного конфликта, с одной стороны, выступает КСС, а с другой – система РЭП противника. В задачу РЭП входит обнаружение сигнала, создание преднамеренных помех или несанкционированный доступ к информации. В таких условиях работы КСС должна принимать меры, которые способствуют выполнению ею своих задач за счет алгоритмического и сигнального ресурса. При реализации методов скрытности в условиях радиоэлектронного противодействия необходимо учитывать требования к помехоустойчивости канала связи.

Ентропійний підхід до оцінювання ризику безпеки інформації в кіберпросторі

УДК 004.056.53
Володимир Мохор, Василь Цуркан, Сергій Михайлов
Інститут спеціального зв'язку та захисту інформації Національного технічного університету України «Київський політехнічний інститут», Україна, v.mokhor@gmail.com, v.v.tsurkan@gmail.com, mixserg@bk.ru

Однією з передумов інформаційної діяльності в кіберпросторі є оцінювання ризику. Завдяки цьому здійснюється вибір засобів зменшення його величини до прийнятного значення та, як наслідок, забезпечується безпека інформації. Ризик визначається як комбінація двох агрегованих оцінок, а саме: величини негативних наслідків (збитків) і ймовірності нанесення цих збитків, тобто ймовірності реалізації загрози. Тоді як загроза представляється парою (джерело, вразливість). Кожен з цих компонентів характеризується своїми частотними та часовими показниками. Тому, зважаючи на багатоманітність факторів, які необхідно враховувати при оцінюванні ризику, варто зазначити, що невизначеності в цих факторах більше, ніж статистичної визначеності. Як наслідок, для врахування впливу невизначеності на забезпечення безпеки інформації в кіберпросторі доцільно використати ентропійний підхід до оцінювання ризику.

У відповідності з цим підходом збитки розглядаються як дискретна випадкова величина, мірою невизначеності якої є ентропія

$$H = -\sum_{i=1}^{n} p_i(x_i) \log_a p_i(x_i), \tag{1}$$

$$\sum_{i=1}^{n} p_i(x_i) = 1, \tag{2}$$

де $p_i(x_i)$ – імовірність реалізації загрози, що призводить до нанесення збитку x_i, $x_i \geq 0$; n – кількість загроз; a – основа логарифму, наприклад: $\log_2(a=2)$, $\lg(a=10)$, $\ln(a=e)$.

Разом з тим, на практиці використання (1) ускладнене необхідністю формування повної групи ймовірних збитків з урахуванням умови нормування (2). Внаслідок цього вони виражаються через неперервну випадкову величину з ентропією

$$H = -\frac{1}{2}\int_{0}^{+\infty} p(x) \log_a p(x) dx, \tag{3}$$

де $p(x)$ – функція щільності розподілу збитків x, $x \in (0,+\infty)$, побудова якої залежить від достатнього обсягу статистичних даних.

Подолання означених обмежень для (1) і (3) можливе завдяки використанню «не ймовірнісної», а нечіткої ентропії. Це дозволить на її основі побудувати інтуїтивно більш коректну базу оцінювання ризику для вибору засобів зменшення його величини до прийнятного значення та, як наслідок, забезпечити безпеку інформації в кіберпросторі.

Концепція «глибокого захисту» корпоративної мережі

УДК 004.7.056.53

Станіслав Ревко
Національний технічний університет України «КПІ», Україна,
stas.revko@gmail.com

Вступ

Способи захисту інформації в корпораційних мережах безперервно змінюються. З постійною появою нового програмного забезпечення, яке швидко становиться необхідним для ефективного функціонування й діяльності підприємства, з'являється ще більше нових вразливостей, що дає можливість зловмиснику реалізовувати загрози великою кількістю різноманітних шляхів.

Оскільки великий список можливих атак постійно поповнюється, то жоден сучасний програмний продукт не може попередити всі атаки самостійно. Виникає потреба в комплексному рішенні побудови системи захисту.

Найкращі результати в умовах малих ресурсних затрат показує концепція «глибокого захисту». Сенс її полягає в тому, що для забезпечення необхідного рівня захищеності потрібно використовувати різні по своїй природі та направленості програми для захисту. Подальше їхнє концептуальне групування та налагодження в середині кожної групи взаємодії та зв'язків створює так звані «лінії захисту».

Централізований збір інформації в реальному часі з кожної лінії захисту утворює синергію системи захисту. Саме взаємодія всіх програм між собою створює рівень захисту, що значно перевершує рівень, який би був досягнутий простим використанням цих же програм без взаємодії.

Міжмережеві екрани (Фаєрвол)

Розглядаючи систему ззовні, першою з головних ліній захисту є мережеві екрани. Їх основне завдання - фільтрація трафіку і блокування несанкціонованого доступу до пристрою, комп'ютера або інших ресурсів корпоративної мережі. Міжмережевий екран має недоліки: по-перше, не захищає вузли мережі від проникнення через «люки» або уразливості ПЗ;•по-друге, не забезпечує захист від багатьох внутрішніх загроз, в першу чергу - витоку даних; по-третє, не захищає від завантаження користувачами шкідливих програм, в тому числі від вірусів. Попри слабкі сторони міжмережеві екрани можуть серйозно підвищити рівень безпеки.

Персональний мережевий екран (Брандмауер)

Частину задач безпеки, що не може виконати фаєрвол, бере на себе персональний мережевий екран. Брандмауер - програмне забезпечення, яке здійснює контроль мережевої активності комп'ютера, на якому він встановлений, а також фільтрацію трафіку відповідно до заданих правил. На відміну від фаєрвола, персональний брандмауер встановлюється безпосередньо на захищаємий комп'ютер, що дозволяє здійснити контроль за конкретними програмами, процесами, й портами відповідного комп'ютера.

Системи виявлення та попередження вторгнень

Системи виявлення та попередження вторгнень (IPS, IDS) є додатковим елементом при побудові системи, що забезпечує безпеку мережі чи

комп'ютерної системи. До них відносяться безліч різних програмних і апаратних засобів, що об'єднуються однією загальною властивістю - аналізують використання довірених їм ресурсів і, в разі виявлення будь-яких підозрілих або просто нетипових подій, здатні робити деякі самостійні дії по виявленню, ідентифікації і усуненню їх причин. Такі системи здатні компенсувати велику кількість різноманітних вразливостей програмного забезпечення і завчасно попередити про ймовірність реалізації загрози.

Антивірусний захист

Хоч використання мережевих і міжмережевих екранів дають можливість значно підвищити рівень захищеності мережі, але вони не можуть забезпечити протидію шкідливим програмам, які вже потрапили в систему, наприклад вірусам.

Одночасно зі створенням власних копій, віруси можуть завдавати значної шкоди: знищувати, пошкоджувати, викрадати дані, знижувати або й зовсім унеможливлювати подальшу працездатність операційної системи комп'ютера.

Саме тому антивірусне програмне забезпечення є також одним із основних рубежів захисту для більшості сучасних підприємств.

Насамперед антивірусні програми націлені на клієнтські пристрої та робочі станції. Вони сканують всі файли, програми, процеси, що знаходяться у постійній чи оперативній пам’яті і перевіряють їх на зараженість вірусом.

Системи моніторингу подій

Система моніторингу подій інформаційної безпеки (ІБ) є одним з основних елементів системи інформаційної безпеки підприємства (відповідно до вимог міжнародних стандартів ISO 27001 та ISO 27002). Водночас вона слугує ключовим елементом підходу «глибокого захисту».

Основою задачею цих систем є централізоване накопичення максимальної кількості інформації про інциденти в системі, що торкаються безпеки. Тобто всі програмні продукти, які тим чи іншим чином впливають на рівень безпеки. Саме це дає можливість її структурувати, систематизувати й проаналізувати на більш якіснішому рівні. Аналіз даних від антивірусу та декількох IDS може виявити загрозу, яка б не виявилася кожним із цих програмних рішень окремо.

Новітні системи моніторингу подій дозволяють вже не тільки спостерігати за подіями, а й запускати механізми штучного інтелекту. Завдяки цьому система захисту побудована на концепції описаній в даній статті зможе самонавчатися, та покращувати реагування на ймовірнісні загрози.

Висновки. Враховуючи широкий спектр можливих загроз на корпоративну мережу, які існують сьогодні, виникає потреба в комплексному рішенні побудови системи захисту. Використовуючи незначні ресурси, найкращий результат показує концепція «глибокого захисту».

Міжмережеві та мережеві екрани, системи виявлення та попередження вторгнень, антивірусні та інші програмні продукти, що торкаються безпеки являють собою окремі рубежі захисту цінної інформації. Системи моніторингу подій забезпечують взаємодію всіх елементів безпеки, чим створюють більш якісний рівень захищеності корпоративної мережі.

Науковий керівник — м.н.с. Хнигічева Альона Михайлівна

Соціоінженерний аспект негативного інформаційно-психологічного впливу на людину в кіберпросторі

УДК 004.056.53

[1] Володимир Мохор, [2] Оксана Цуркан
[1] Інститут спеціального зв'язку та захисту інформації Національного технічного університету України «Київський політехнічний інститут», Україна, v.mokhor@gmail.com, [2] Центр науково-технічної інформації та сприяння інноваційному розвитку України, Україна, o-v-c@yandex.ru

Одним із аспектів розгляду негативного інформаційно-психологічного впливу є використання уразливостей людини за допомогою соціальної інженерії (рис.1). Маніпулювання ними дозволяє отримати несанкціонований доступ до інформації без руйнування та перекручування головних для неї системоутворюючих якостей. З огляду на це, використання соціальної інженерії є однією з найбільш розповсюджених загроз безпеці інформації в кіберпросторі.

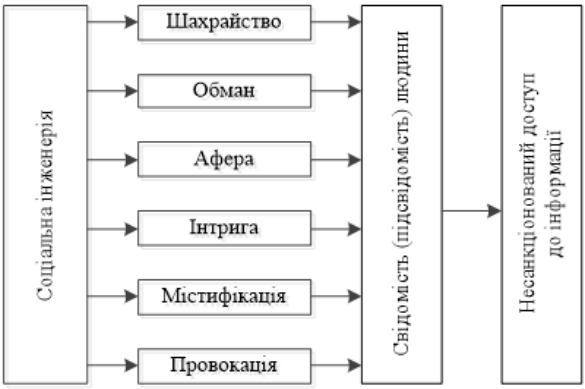

Рис. 1. Сутність використання соціальної інженерії

З огляду на рис. 1, реалізація цієї загрози передбачає цілеспрямований вплив на свідомість (підсвідомість) людини проти волі, але за її згодою. Такий вплив дозволяє управляти людською поведінкою через слабкості, інтереси, потреби, схильності, переконання, звички, психічний та емоційний стан. Маніпулювання цими уразливостями виражається в таких формах як, наприклад, шахрайство, обман, афера, інтрига, містифікація, провокація. Разом з тим, використанню кожної з означених форм маніпулювання передує визначення його змісту шляхом ретельних планування, організації та контролювання.

Таким чином, розгляд негативного інформаційно-психологічний впливу на людину в соціоінженерному аспекті дозволить врахувати особливості використання маніпулятивних форм для несанкціонованого доступу до інформації та, як наслідок, запобігти реалізації загрози використання соціальної інженерії в кіберпросторі.

Вибір парольних параметрів фрактальної схеми автентифікації

УДК 003.26 : 004.056.53
Денис Самойленко
Національний університет кораблебудування, Україна, denniksam@gmail.com

Особливі властивості фрактальних утворень дозволили висловити пропозицію щодо їх використання у захисних цілях як для матеріальних носіїв інформації [1], так і для автентифікаційних протоколів за принципом нульового розголошення [2]. Головним секретом (паролем) фракталу виступає набір числових параметрів, встановлених для його побудови. Дана робота присвячена дослідженню якісних показників безпеки фрактальної схеми автентифікації для різних варіантів вибору паролів.

Автентифікаційна схема ґрунтується на перевірці узгодженості у різних сторін числових величин C=(ReC, ImC) та N, шляхом обміну даними щодо збіжності послідовності

$$X_{k+1} = (X_k)^N + C \qquad (1)$$

для різних, випадково обраних точок X_0. Встановлено, що незначні відмінності у значені C призводять до суттєвих змін області збіжності послідовності.

Слід зазначити, що при програмній реалізації протоколу, збіжність послідовності перевіряється шляхом утворення циклу з двома умовами виходу: одна відповідає зростанню модуля X до межі розбіжності, друга обмежує кількість ітерацій обчислення послідовності (1).

Множина усіх точок, для яких послідовність (1) збігається утворює множину Мандельброта [3]. Досліджуючи образи фрактальних множин, що відповідають різним областям множини Мандельброта можна дійти висновку, що найбільшу чутливість до значення константи C демонструють множини, побудовані для пограничних точок. При цьому самі фрактальні образи стають сильно розрідженими і являють собою сукупність окремих точок. Навпаки, для внутрішніх точок множини Мандельброта фрактальні образи є суцільними, з чітко відокремлюваними областями збіжності. При змінах C спостерігається відносно незначна зміна границі фракталу.

Експериментальне визначення кількості помилок автентифікації дозволило встановити наступні значення: для паролю C=(0,24; 0,50), N=2 (внутрішня точка множини Мандельброта) при відхиленні однієї складової C на 0,01 спостерігається близько 24 помилок на 1000 запитів, при відхиленні на 0,001 – 3-4 помилки. У той же час для паролю C=(0,59; 0,42), N=3 (точка, близька до граничної), при відхиленні на 0,01 утворює 70-80 помилок автентифікації на 1000 запитів, при відхиленні на 0,001 – 22-24 помилки.

Підвищення ступеня N дозволяє покращити показники надійності. Так, для паролю C=(0,61; 0,45), N=4 (точка, дещо віддалена від граничної) при відхиленні на 0,01 виявляється 71-75 помилок на 1000 запитів, при відхиленні на 0,001 – 19-20 помилок. Усі експерименти проводились для рівномірного розподілу імовірності вибору точки X_0 у потенційному просторі збіжності.

Підсумовуючи результати експериментів можна сформулювати рекомендацію щодо вибору у якості парольних параметрів значення, близькі до граничних точок множини Мандельброта та, за можливості, високі ступені

перетворення (1). Окремо слід відзначити, що мова іде про граничні точки множини, що відповідає заданому значенню ступеня *N*, оскільки класично вважається, що *N*=2.

Вибір граничних точок супроводжується посиленням чутливості фрактального образу до кількості ітерацій, що реалізуються для перевірки збіжності. Прояв стохастичного перемішування призводить до того, що найменші флуктуації призводять до глобального ефекту (зміни характеру збіжності), проте для цього може знадобитись значна кількість ітерацій обчислення послідовності (1). Чим ближче обрана точка до межі множини Мандельброта, тим швидше проявляється зазначений ефект.

На рис. 1 наведені образи фрактальної множини, побудованої для різних значень кількості ітерацій. Як можна помітити, збільшення кількості ітерацій призводить до розрідження через прояв відхилень у «віддаленій еволюції».

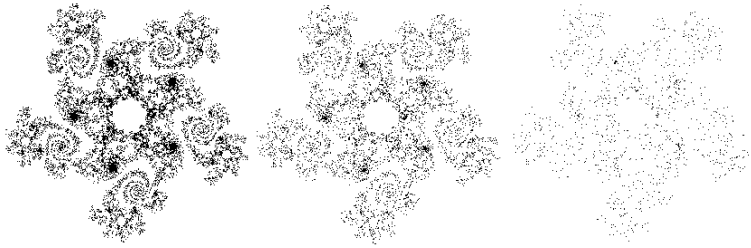

Рис. 1. Образи фрактальної множини *C*=(0,245; 0,70), *N*=5 для кількості ітерацій 200, 300, 500 (зліва направо).

Зазначена поведінка фрактальної множини вимагає обов'язкового встановлення однакової граничної кількості ітерації у програмних кодах клієнта та сервера. З іншого боку, описана особливість може бути використана для корегування змісту автентифікаційного пароля. Окрім наведених вище числових констант, до складу секрету може бути додана величина, що визначатиме умову виходу з програмного циклу.

Висновки: надано рекомендацію вибору паролів фрактальної схеми автентифікації близько до граничних точок множини Мандельброта та з високими ступенями перетворень. Запропоновано долучити до складу паролю кількість ітерацій послідовності. Оцінено величини помилок автентифікації для різних відхилень паролю.

Література: 1. Самойленко Д. М. Використання фрактальних зображень для голографічного захисту поліграфічної продукції [Текст] / Самойленко Д. М., Мірошниченко О. В. Попов Д. Д. // Квалілогія книги. – 2010. – № 2 (18). – с. 77-81. 2. Самойленко Д. М. Використання фрактальних множин у протоколах з нульовим розголошенням [Текст] / Самойленко Д. М. / Матеріали III Всеукраїнської науково-практичної конференції з міжнародною участю «Сучасні проблеми інформаційної безпеки на транспорті». – Миколаїв: Вид-во НУК, 2013. – с. 92-95. 3. Mandelbrot B. Fractals and Chaos. [Текст] / Mandelbrot B. – Berlin: Springer. – 2004 – p. 38.

Програмний комплекс криптографічних систем шифрування

УДК 004.056.55 (003.26)

[1] Олександр Корченко,
[2] Юрій Дрейс, [2] Володимир Сіденко
[1] Національний авіаційний університет, Україна, icaocentre@nau.edu.ua,
[2] Житомирський військовий інститут імені С.П. Корольова
Державного університету телекомунікацій, Україна,
dr_yr_al@mail.ru, sidenkovladimir52@mail.ru

Результатом цілеспрямованої сумісної діяльності співробітників кафедри безпеки інформаційних і комунікаційних систем Житомирського військового інституту ім. С.П. Корольова Державного університету телекомунікацій та кафедри безпеки інформаційних технологій Національного авіаційного університету щодо вдосконалення навчальних планів і програм підготовки фахівців, які володіють сучасними інформаційними технологіями у галузі знань 1701 «Інформаційна безпека», є підготовлений підручник «*ПРИКЛАДНА КРИПТОЛОГІЯ: системи шифрування*» для забезпечення навчально-методичного комплексу дисциплін «Прикладна криптологія» та «Основи криптографічного захисту інформації» за вимогами освітньо-кваліфікаційних характеристики та освітньо-професійної програми.

Метою даного підручника є навчання студенів принципам побудови систем захисту інформації на основі використання простих та сучасних алгоритмів симетричного й асиметричного шифрування для забезпечення конфіденційності даних в інформаційно-телекомунікаційних системах (ІТС).

Слід відмітити, що до підручника додається *компакт диск* (CD-R) на якому міститься у достатній кількості комп'ютерні програми шифрування даних сучасних криптографічних алгоритмів з можливостями покрокової демонстрації візуалізації процесів зашифрування / розшифрування, на які отримані авторські свідоцтва – *програмний комплекс криптографічних систем шифрування* (рис. 1). Також на диску є електронна версія підручника у форматі .pdf й додаткові програми функціонального призначення.

Рис. 1. Програмний комплекс криптографічних систем шифрування

Відповідно до мети підручника, програмний комплекс криптографічних систем шифрування для забезпечення конфіденційності даних в ІТС містить такі основні *комп'ютерні програми* як:

1. «Програма візуалізації процесу забезпечення конфіденційності даних з використанням стандарту криптографічного перетворення ГОСТ 28147-89 у режимі гамування» (програмний продукт, що має одномодульну структуру з можливостями покрокової візуалізації (демонстрації) процесу забезпечення конфіденційності при шифруванні/розшифруванні даних з налаштуванням параметрів та дослідженням алгоритму криптографічного перетворення даних ГОСТ 28147-89);

2. «Програма візуалізації процесів забезпечення конфіденційності даних в ІТС з клієнт-серверною організацією зв'язку при використанні алгоритму симетричного шифрування Data Encryption Standard (DES)» (програмний продукт з клієнт-серверною організацією зв'язку та з можливостями візуалізації (демонстрації) процесів: налаштування параметрів криптосистеми; покрокового забезпечення конфіденційності при шифруванні/розшифруванні даних алгоритмом симетричного шифрування DES та передачі їх між абонентами (клієнтами) ІТС);

3. «Програма візуалізації процесу забезпечення конфіденційності даних з використанням блочного симетричного шифру Advanced Data Encryption (ADE)» (програмний продукт з можливостями візуалізації (демонстрації) процесів: створення та налаштування загальних параметрів криптосистеми; забезпечення конфіденційності при шифруванні/розшифруванні даних блочним симетричним шифром ADE);

4. «Програма візуалізації процесів забезпечення конфіденційності даних в ІТС з клієнт-серверною організацією зв'язку при використанні алгоритму симетричного шифрування Triple Data Encryption Standard (3 DES)» ();

5. «Програма шифрування даних крипторгафічним алгоритмом IDEA з покроковою візуалізацією процесів» (програмний продукт з покроковою візуалізацією процесів забезпечення конфіденційності при шифруванні /розшифруванні даних криптографічним алгоритмом IDEA у режимах роботи: з одним блоком даних (64 біти) та з файлом даних довільної довжини);

6. «Програма візуалізації процесу забезпечення конфіденційності даних з використанням блочного симетричного шифру RIJNDAEL» (програмний продукт з візуалізацією (демонстрацією) процесів: налаштування параметрів криптосистеми (секретного ключа, вхідних даних); покрокового забезпечення конфіденційності при шифруванні/розшифруванні даних шифром RIJNDAEL в режимі Electronic Codebook та формування раундових ключів;

… та інші програми.

Наступне видання буде присвячене вивченню алгоритмів та стандартів симетричного і асиметричного шифрування для забезпечення автентичності й цілісності даних в ІТС, а також блоковим симетричним шифрам національного конкурсу України з розробкою авторського програмного комплексу систем автентифікації, хешування та електронного цифрового підпису (на прикладі, ГОСТ Р 34.11-94, MD 5, Лабіринт, RIPEMD-160 та DSA, Мухомор та інші) у якості додатку – компакт диску.

Особливості впровадження ділових ігор у процес навчання фахівців з інформаційної безпеки

УДК 004.056(681.58)

[1]Юрій Копитін, [2]Сергій Стайкуца
[1] КП «Обласний інформаційно-аналітичний центр», м. Одеса, Україна, ykopitin@odessa.gov.ua, *[2] Одеська національна академія зв'язку ім. О.С. Попова, Україна,* s_t_a@ukr.net

Забезпечення належного рівня інформаційної безпеки напряму залежить від якісної професійної підготовки майбутніх фахівців, рівня впровадження та використання інноваційних педагогічних, інформаційно-комунікаційних технологій та формування інформаційної культури. У наукових виданнях, засобах масової інформації, в мережі Інтернет, на науково-практичних конференціях, семінарах, круглих столах широко обговорюються відомості про стан, проблеми, особливості, організаційні, науково-методологічні аспекти та теоретико-методичні основи підготовки фахівців з інформаційної безпеки. Однак особливості впровадження у навчання фахівців з інформаційної безпеки ділових ігор розкрито недостатньо.

В зв'язку з чим, *метою роботи* є презентація результатів впровадження ділових ігор у процес навчання фахівців з інформаційної безпеки в Одеській національній академії зв'язку ім. О.С. Попова.

В умовах ринкової економіки випускникам вищих навчальних закладів необхідно мати не лише теоретичні знання, а й потрібно вміти працювати в команді, мати культурні, мовні, комунікативні навички. Як відомо, ділові ігри є одним із ефективних методів навчання, який сприяє набуттю заданих компетенцій, а саме забезпечує імітацію спільної діяльності людей, імітацію прийняття управлінських рішень в різних виробничих ситуаціях, іноді досить нестандартних, у режимі інтерактивного діалогу.

Для перевірки ефективності використання ділових ігор у процесі підготовки фахівців з інформаційної безпеки за участю студентів 4 курсу, які навчаються за спеціальністю 6.170102 «Системи технічного захисту інформації», було апробовано ділову гру на тему «Організація процесу створення комплексної системи захисту інформації в автоматизованій системі 1 класу (комп'ютер відділу бухгалтерського обліку Департаменту освіти та науки облдержадміністрації, призначений для обробки персональних даних)». Метою гри є розвиток у студентів навичок з самостійного виконання робіт із створення комплексної системи захисту інформації (КСЗІ) в автоматизованій системі 1 класу (АС-1).

Завдання ділової гри: - навчитись застосовувати положення нормативно-правових актів з питань захисту інформації в інформаційно-телекомунікаційних системах; - навчитись вести діалог з колегами, спрямований на укладання договору, накопичення відомостей про АС-1, отримання відомостей про заходи та засоби захисту в АС-1; - навчитись проводити роботи з обстеження АС-1, побудови моделі загроз, формування вимог до КСЗІ та вибору комплексу засобів захисту, обирати засоби та заходи захисту, проходити державну експертизу КСЗІ АС-1.

У діловій грі процес створення КСЗІ в АС-1 здійснюється на основі заданих викладачем характеристик. Функціональна діаграма гри (рис. 1) відтворює послідовність виконання функцій для розгляду задачі створення комплексної системи захисту інформації. Розроблений сценарій ділової гри розрахований на 4 академічних години та групу студентів від 18 до 25 осіб.

Рис. 1. Функціональна діаграма гри

Критеріями оцінки рівня знань під час гри є: - глибина та рівень опрацювання завдання; - ступінь знання нормативної документації та засобів захисту інформації; - рівень логічності та обгрунтованості запропонованих рішень щодо створення КСЗІ в АС-1; - своєчасність виконання завдань; - аргументованість прийнятих рішень у ході дискусії.

За результатами проведення гри студентам поставлено оцінки у бальній шкалі. Для перевірки коректності критеріїв оцінки рівня знань студентів додатково проведено оцінювання студентів у формі тестування. Результати оцінювання за підсумками ділової гри та шляхом проведення тестування збіглися. Зазначимо, що в порівнянні з минулими роками, отримано на 30% кращі результати. Отже, ділові ігри можуть бути використані для проведення контролю рівня знань студентів. При цьому контроль здійснюється безпосередньо в процесі гри, що дозволяє скоротити час на його проведення.

На відміну від попередніх років, коли зазначений матеріал подавався виключно традиційними методами, під час виконання студентами задач виробничої практики встановлено, що якість засвоєння матеріалу зросла з 20 (двадцять) % до 80 (вісімдесят) %. Після участі у діловій грі, студенти мали чітку уяву про заходи, які виконуються під час створення КСЗІ в АС-1.

Основною перевагою використання ділових ігор у навчальному процесі є те, що вони не заміняють традиційні методи навчання, а раціонально їх доповнюють, дозволяючи більш ефективно вирішувати поставлені завдання.

Як висновок, зазначимо, що продемонстровані результати підтверджують, що завдяки використанню ділової гри у навчальному процесі, студенти краще закріплюють здобуті теоретичні знання, глибше пізнають предмет навчання, а також отримують певні практичні навички.

Побітове приховування даних у SVG зображення на основі кривих Без'є

УДК 003.26:004.056.5

Олексій Кінзерявий
Національний авіаційний університет, Україна, oleksiykinzeryavyy@gmail.com

Стеганографія – це наука, що вивчає засоби захисту інформації шляхом приховування даних у інших об'єктах (контейнерах), використовуючи при цьому їх структурні особливості побудови. Так, в векторні зображення формату *SVG*, завдяки використання в них кривих Без'є, можна приховати інформацію. Метою даної роботи є опис процесу приховування даних у *SVG* зображення.

Приховування в *SVG* зображення здійснюється шляхом розбиття кривих Без'є на візуально однакові під криві (сегменти). Процес приховування та вилучення даних з *SVG* зображення можна поділити на наступні етапи: 1) аналіз векторного зображення на використання кривих Без'є при побудові векторних об'єктів; 2) приховування даних шляхом розбиття кривих Без'є на під криві; 3) вилучення даних з обробленого векторного зображення шляхом відтворення початкової кривої.

1. Проведення аналізу векторного зображення на використання кривих Без'є при побудові векторних об'єктів виконується з метою визначення в ньому необхідних структурних елементів, що дадуть можливість здійснити приховування даних у вибраному *SVG* зображенні. До таких ключових елементів відноситься об'єкт *Path* та використовувані в ньому команди побудови кривих Без'є типу: curveto (C / c), smooth curveto (S / s), quadratic Bezier curveto (Q / q) і smooth quadratic Bezier curveto (T / t).

2. Приховування даних в векторне зображення здійснюється шляхом поступового розбиття кривої Без'є на під криві за алгоритмом де Кастельжо при використанні параметра побудови кривої t, що змінюється з довільним кроком dt в межах $0 \le t \le 1$. Визначивши певний крок dt можна здійснити приховування інформації за наступними правилами: якщо на певному кроці t приховується біт з значенням «0», то при даному t крива Без'є не ділиться і відбувається перехід до наступного значення $t = t + dt$; якщо при певному значенні t потрібно приховати біт з значенням «1», то на даному значенні t відбувається розбиття кривої Без'є на дві під криві, що візуально будуть однакові початковій кривій, і відбувається перехід до наступного значення $t = t + dt$. Причому, подальше приховування даних відбуватиметься в одержану другу під криву.

Розбиття кривої типу *curveto* на певному кроці t за алгоритмом де Кастельжо проходитиме в три кроки, де на кожному кроці обраховуються додаткові точки: 1) з початкових координат P_0, P_1, P_2, P_3 точок кривої Без'є обраховуються координатами точок P_0^1, P_1^1, P_2^1. 2) з отриманих координат точок P_0^1, P_1^1, P_2^1 обчислюються наступні додаткові точки P_0^2 та P_1^2. 3) з отриманих

координат точок P_0^2, P_1^2 обчислюються координати останньої шуканої точки P_0^3. З обчислених координат додаткових точок будуються дві криві Без'є, де перша крива будується по точках P_0, P_0^1, P_0^2, P_0^3, а друга крива – P_0^3, P_1^2, P_2^1, P_3.

3) Вилучення даних з обробленого векторного зображення відбувається шляхом відтворення початкової кривої. Відтворення здійснюється у поступовому об'єднанні двох останніх кривих послідовності з приховуваними даними, поки не буде відтворена початкова крива. Об'єднання двох останніх кривих відбувається за наступними правилами: 1) На кожному кроці t обчислюються координати точок P_1^1 за двома способами: а) обраховуються додаткові координати P_1 та P_2, за допомогою яких обраховується координати точки $P_{1(1)}^1$; б) за координатами P_1^2 та P_2^1, що беруться з кінцевих кривих, обраховуються координати точок $P_{1(2)}^1$. 2) Якщо значення $P_{1(1)}^1$ та $P_{1(2)}^1$ при можливій похибці Er однакові ($P_{1(1)}^1 \approx P_{1(2)}^1$), то на даному кроці t відбуватиметься об'єднання двох кривих в одну криву Без'є, що надалі буде поєднуватися з наступною кривою Без'є послідовності при наступному значені $t = t + dt$. Таке об'єднання кривих вказуватиме на отримання біта приховуваної послідовності з значенням «1». 3) Якщо рівність $P_{1(1)}^1 \approx P_{1(2)}^1$, при можливій похибці Er, не виконується, то дані криві будуть порівнюватися знову при наступному кроці $t = t + dt$, а це означатиме отримання біта приховуваної послідовності з значенням «0».

Результати побітового приховуванню даних в одну криву Без'є при використанні довільних *SVG* зображень наведені в табл. 1. Приховування даних здійснювалося з використання наступних параметрів: $Dp = 15$, де Dp – максимально допустима кількість знаків дробової частини при обчисленнях; $Er = 10^{-10}$.

Табл. 1. Побітове приховування даних у *SVG* зображення

Номер *SVG* файлу	Загальна кількість кривих Без'є	Розмір прихованої інформації, байт	Розмір контейнеру «до», байт	Розмір контейнеру «після», байт	Збільшення розміру контейнера, %
1	197	100	18949	66146	249,07
2	1064	200	69428	160895	131,74
3	130	300	10019	147083	1368,04
4	109	400	8643	190844	2108,08
5	922	500	63636	290914	357,15

Отримані результати побітового приховування даних у *SVG* зображення показує досить гарні результати, що можна покращити шляхом приховування даних у всі криві Без'є векторного зображення. Однак, недоліком такого приховування є значне збільшення розмірів *SVG* контейнера.

Модель вероятностной надежности комплекса технической защиты информации с учетом стоимости и параметров взлома

УДК 004.056.5(043)

Борис Журиленко
Национальный авиационный университет, Украина, zhurilenko@mail.ru

Современный этап создания комплекса технической защиты информации (КТЗИ) основывается, в основном, на статистических данных не связанных с динамикой непосредственного их развития во времени. При организации технической защиты, заказчика, в первую очередь, будет интересовать стоимость и эффективность применения того или иного комплекса защиты во времени, так как в условиях эксплуатации больший интерес представляет защита информации не столько в статике, сколько в динамике, то есть во времени.

В настоящие время существует хорошо разработанная методика расчета надежности радиоэлектронных устройств и оборудования, которая реально обеспечивает необходимый уровень надежности на отказ. Если использовать эту методику для разработки методологии защиты информации, то появляется возможность предсказать, когда уровень защиты уже недостаточен и КТЗИ требует модернизации или замены. Такой подход позволит сэкономить финансовые ресурсы при проектировании, провести исследования и анализ свойств КТЗИ, выработать рекомендации для его модернизации или новые требования для его разработки. Обеспечение выполнения всех перечисленных выше возможностей анализа, исследования и проектирования комплекса защиты требует разработки методологии на основе вероятностной математической модели КТЗИ во времени и с учетом его стоимости.

Целью данной работы являлось создание вероятностной математической модели надежности КТЗИ, которая давала бы количественную оценку надежности того или иного КТЗИ во времени с учетом его стоимости и обеспечивала бы возможность сравнения теоретических результатов с реальными практическими результатами взлома.

В основу построения вероятностной математической модели надежности КТЗИ положены следующие соотношения:

1. В случае если устройство работоспособно только при работоспособном состоянии всех его элементов, то вероятность работоспособности устройства, будет определяться выражением

$$P_{раб} = \prod_{i}^{N} p_i \,. \tag{1}$$

2. В случае, если отказ устройства наступает только тогда, когда отказывают все его элементы, то вероятность отказа будет иметь вид

$$P_{отк} = 1 - \prod_{i}^{N} (1 - p_i) \,, \tag{2}$$

где N – количество элементов, обладающих вероятностью безотказности p_i.

Воспользуемся выражениями для максимума вероятности взлома от вложенного финансирования на его защиту. Обозначим через $X_i = x_i / H_i$ – приведенные вложения финансов на каждую из защит; x_i – финансовые

затраты на создание ТЗИ; H_i – первоначальные финансовые потери при отсутствии защиты; β_i – определяет эффективность защиты от вложенного финансирования на ее построение. Индекс i указывает на то, что данный параметр относится к i-той защите.

$$P_i(X_i) = [\frac{X_i^{X_i}}{(1+X_i)^{1+X_{i_1}}}]^{\beta_i}, \quad (3)$$

Из опубликованных результатов возьмем максимум вероятности взлома во времени в виде

$$P_i(m,t) = [(\frac{f_i(m,t)}{f_i(m,t)+t})^{\frac{f_i(m,t)}{t}} \cdot (\frac{t}{f_i(m,t)+t})]^{\gamma_i}, \quad (4)$$

где $f_i(m,t)$ – параметр, присущий данной i-той системе защиты, и который может быть определен только из реальных результатов или проектируемых параметров взлома защиты и времени этого взлома; t – текущая координата времени; γ_i – определяет эффективность i-той защиты во времени.

Используя уравнения (1) – (4) получим выражение для вероятности взлома КТЗИ

$$P_{взлКТЗИ}(X_i, m, t) = \prod_{i=1}^{n}\{1-[1-P_i(X_i)]\cdot[1-P_i(m,t)]\}^{\alpha_i}, \quad (5)$$

где $P_i(m,t)$ - вероятность взлома, определяемая попыткой взлома и временем этой попытки взлома, α_i - эффективность i-той защиты, n – количество, применяемых защит.

И окончательно получим формулу математической модели вероятностной надежности КТЗИ

$$P_{защКТЗИ}(X_i, m, t) = 1 - \prod_{i}^{n}\{1-[1-P_i(X_i)]\cdot[1-P_i(m,t)]\}^{\alpha_i}. \quad (6)$$

В результате проделанной работы можно сделать следующие выводы. Полученное выражение показывает, что если нет финансовых вложений в защиту или ее модернизацию, то вероятность надежности защищенности равна нулю независимо от времени взлома. В начальный момент времени при $t=0$ ТЗИ соответствует вероятности защищенности только за счет вложенного финансирования на защиту или модернизацию. Если рассматривать вероятность защищенности от максимально эффективного вложения финансирования, то она равна трем или менее финансовым потерям без защиты. Получено общее выражение, позволяющее определять вероятности любых событий во времени. Для этого в общем выражении (6) вероятность финансовых затрат на КТЗИ заменяется вероятностью рассматриваемого события в начальный момент времени $t=0$. Временная вероятность остается в том же виде, но из экспериментальных исследований или реальных событий взлома или защищенности определяются параметры, отвечающие за взлом. Если в защищенности участвуют различные вероятностные процессы, то в этом случае общая вероятность защищенности будет определяться как для комплекса технической защиты информации с помощью выражения (6).

Метод оцінки нейромережевих засобів щодо можливостей виявлення інтернет-орієнтованих кібератак

УДК 681.3.06

[1] Олександр Корченко, [2] Ігор Терейковський
Національний авіаційний університет Україна,
agkorchenko@mail.ru, terejkowski@ukr.net

Однією із основних тенденцій вдосконалення сучасних систем виявлення атак є застосовування методів теорії штучних нейронних мереж. Хоча ефективність нейромережевих засобів вважається доведеною, однак сфера їх застосування визначена недостатньо чітко. Особливо актуальним є питання окреслення множини Інтернет-орієнтованих кібератак, котрі слід розпізнати. Це обмежує ускладнює процес створення систем виявлення та призводить до збільшення кількості хибних спрацювань. Тому метою даної роботи є розробка методу оцінки нейромережевих засобів щодо можливості виявлення Інтернет-орієнтованих кібератак. Вказаний складається із наступних етапів:

1. Оцінити можливість отримання статистичних даних, які можна використати для навчання НМ, призначеної для виявлення атак певного типу.
2. Визначити номенклатуру вхідних та вихідних параметрів НМ.
3. Визначити допустиму помилку та допустимий термін навчання НМ.
4. Визначити архітектуру НМ.
5. Розрахувати мінімально допустиму кількість навчальних прикладів: $P_{\min} \geq (10..20)N_x$, де N_x – кількість вхідних параметрів НМ.
6. Розрахувати термін навчання НМ (t) на P_{min}. Для карти Кохонена, мережі PNN та РБФ, $t \approx 0{,}1\tau e^{-\varepsilon} P(N_X + N_Y)$, де P – кількість навчальних прикладів, ε – допустима помилка навчання, τ – тривалість однієї обчислювальної операції, N_Y – кількість вихідних параметрів. Для багатошарового персептрону $t \approx 0{,}001\tau e^{-\varepsilon} P^2 (N_X + N_Y)^2$.
7. Оцінити можливість навчання НМ на P_{min} за допустимий термін навчання.
8. Визначити максимально допустиму тривалість розробки НМ: $T_f \leq T_a$, де T_a – термін, на протязі якого ризик від реалізації атаки допустимий.
9. Розрахувати максимально допустимий термін формування навчальної вибірки: $T_{\max} = T_f - t$, де t – термін навчання НМ.
10. За допомогою експертних даних оцінити можливість формування мінімально допустимої навчальної вибірки за термін T_{max}.
11. Застосовувати НМ доцільно при позитивних оцінках 8-ого та 11-го етапів.

За допомогою розробленого методу доведена можливість застосування нейромережевих засобів для розпізнавання: Dos-атак, сканування портів, IP-спуфінгу та Веб-орієнтованих вірусів. Таким чином, вперше розроблено метод який дозволяє оцінити можливість застосування нейромережевих засобів для виявлення Інтернет-орієнтованих кібератак. Перспективи подальших досліджень полягають у розробці методу оптимізації параметрів НМ, що використовуються в засобах розпізнавання зазначених кібератак.

Повышение достоверности идентификации видеосистем контроля

УДК 004.056(043.2)
Валериян Швец, Виталий Васянович
Національний авіаційний університет, Україна, hvank21@yandex.ua, vasianovichv@ukr.net

В настоящее время всё более широкое распространение получают биометрические системы идентификации человека, которые основываются на уникальных биологических характеристиках человека. Эти характеристики трудно подделать и они однозначно определяют конкретного человека.

Распознавание человека по изображению лица выделяется среди биометрических систем тем, что, во-первых, не требуется специальное или дорогостоящее оборудование, во-вторых, не нужен физический контакт с устройствами.

Система распознавания человека по изображению лица не обеспечивает 100%-ой надёжности идентификации и имеет свои недостатки. Одним из таких недостатков возможность подмены, то есть возможность выдать фотографию за реального человека, что делает систему уязвимой.

Для решения данной проблемы разработан метод определения подлинности человека во время его аутентификации. Суть метода заключается в анализе поведения контрольных точек лица человека.

С анатомической точки зрения, шея человека является точкой опоры для его головы, относительно которой происходит движение всех точек лица. Поэтому, была выдвинута гипотеза о том, что с помощью портрета невозможно воссоздать траекторию движения точек лица реального человека.

Для проверки данной гипотезы был проведен эксперимент, который заключался в сравнительном анализе траекторий движения контрольных точек лица человека при съемке реального человека и при попытке подмены его портретом.

Суть эксперимента заключалась в следующем:

1. С помощью специализированного программного обеспечения осуществляется поиск лица на изображении.
2. Строятся траекторий движения контрольных точек. В качестве контрольных точек лица человека (уголки глаз, уголки рта, центры зрачков).
3. Проводится анализ траекторий движения контрольных точек.

Результаты анализа показали (анализ проводился для последовательности, объемом в 35 кадров с помощью программного обеспечения Matlab R2013a) [2], что траектории контрольных точек лица реального человека отличается от траекторий контрольных точек лица на портрете (рис. 2).

В данный момент проводится разработка автоматизированного алгоритма поиска координат контрольных точек на лице человека и вычисление траекторий. Алгоритм реализован с помощью программного обеспечения OpenCV.

Технологія кодування кортежів трансформованих зображень в інфокомунікаційних системах

УДК 004.056.5

Владимир Баранник, Сергей Туренко,
Виталий Твердохлеб, Али Бекиров
Харьковский университет Воздушных Сил им. Ивана Кожедуба, Украина,
Barannik_V_V@mail.ru

Критичність надання відеоінформаційних послуг пов'язана з проблематичністю щодо забезпечення заданих характеристик по затримці на вузлі доступу, затримці від джерела до одержувача; ймовірності втрати пакетів на вузлі доступу. У зв'язку з чим, необхідно обґрунтувати і розробити технологію кодування в напрямку вдосконалення JPEG платформи. Тут використовується стратегія компонентного кодування квантизованної трансформанти, яка будується з урахуванням таких властивостей як: концентрація основної енергії вихідного сигналу в обмеженій кількості низькочастотних компонент трансформанти; виділення області високочастотних компонент; поява компонент трансформанти з нульовими значеннями. Здійснюється виділення довжин ланцюжків, що складаються з компонент трансформанти, мають після квантизації нульові значення. У результаті формуються двокомпонентні кортежі. Тому пропонується проводити подальший розвиток теоретичних підходів і побудову технологій обробки трансформованих зображень в напрямку кодування векторів двокомпонентних кортежів (ДК). Звідси обґрунтування і створення технології компресії трансформованих зображень на базі кодування векторів двокомпонентних кортежів і визначає мету дослідження статті.

Розробляється модель оцінки кількості інформації в усіченій лініарізованій трансформанті у разі формування вектору двокомпонентних кортежів і виявлення структурних обмежень на динамічний діапазон. Показується, що середня кількість потенційно скорочуваної надмірності, що припадає на один двокомпонентний кортеж, змінюється в межах від 40 до 60 % залежно від ступеня насиченості сегменту зображення. Вперше розроблено математичну модель для оцінки інформативності лініарізованої трансформанти. Відмінні характеристики моделі полягають у тому, що: вектор двокомпонентних кортежів, являє собою двовимірний комбінаторний об'єкт. Це дозволяє оцінити нижню межу ефективності компресії сегментів зображень. Обґрунтовується інтерпретація усіченого вектора двокомпонентних кортежів як укрупненого позиційного числа невизначеної довжини, елементами якого є коди двоелементних біадічних чисел, утворених для окремих двокомпонентних кортежів. Проводиться створення кодостворюючe співвідношення, що забезпечує формування коду для укрупненого позиційного числа з невизначеною довжиною по дворівневій схемі, а саме: на першому рівні формується кодове подання для окремих двокомпонентних кортежів, а на другому рівні здійснюється формування загального кодового представлення для кодів, отриманих на першому рівні.

Анализ актуальных угроз безопасности видеоинформационного ресурса систем видеоконференцсвязи

УДК 004.056.5

Владимир Баранник, Андрей Власов,
Руслан Акимов, Сергей Сидченко
Харьковский университет Воздушных Сил им. Ивана Кожедуба, Украина,
Barannik_V_V@mail.ru

В профильных системах управления специального назначения (Вооруженные Силы, МВД и т.д.) одной из составляющих современного процесса управления и обеспечения объективного контроля является применение систем видеоконференцсвязи (ВКС). При этом показано что, видеоинформационный (ВИ) ресурс ВКС в таких системах управления приобретает значение государственного информационного ресурса. Однако обеспечение безопасности данного ресурса решается в составе единого комплекса мероприятий по обеспечению информационной безопасности в системе управления, без учета оценки уязвимостей и угроз безопасности ВИ ресурса, которые возникают непосредственно в процессе функционирования ВКС. Поэтому повышение безопасности ВИ ресурса при функционировании видеоконференцсвязи в профильных системах управления специального назначения является актуальной научно – прикладной задачей.

В связи с этим требуется разработать модель угроз безопасности ВИ ресурса и выполнить анализ значимых (актуальных) угроз.

Для определения значимых уязвимостей и актуальных угроз безопасности ВИ ресурсу в процессе функционирования ВКС предлагается оценить характеристики ВИ ресурса комплексов ВКС (объем видеоданных, средняя скорость видеопотока, время передачи несжатого видео-потока, битовая скорость сжатого видеопотока и др.). Данная оценка позволит определить соответствие характеристик ВИ ресурса современным требованиям обработки в системах ВКС и доставки видеоинформации в профильных системах управления.

Выполненный анализ оценок характеристик ВИ ресурса и их соответствия технологиям обработки и доставки видеоинформации в профильных системах управления показывает, что:

а) требования субъектов доступа по динамическому изменению (в сторону увеличению) качества видеоданных в процессе сеансов видеоконференсвязи будет приводить к существенному возрастанию объемов видеоданных и как следствие к возникновению дестабилизирующих факторов, приводящих у нарушению безопасности ВИ ресурса ВКС, а именно категорий доступности и целостности;

б) временные задержки при передаче ВИ ресурса для высоких значений пространственных разрешений видеокадров (HD, Full HD, Advantage HD) превышают допустимые значения времени доступа в десятки раз;

в) увеличение степени компрессии видеоданных для уменьшения объема видеопотока приводит к нарушению семантической целостности ВИ ресурса (увеличение искажений в процессе сжатия).

Анализ эффективности технологий шифрования в процессе формирования видеопотока

УДК 004.056.55
Юрий Рябуха, Дмитрий Комолов, Роман Тарнополов
Харьковский университет Воздушных Сил им. Ивана Кожедуба, Украина, Barannik_V_V@mail.ru

Процессы обработки и передачи данных в современных инфокоммуникационных системах включают в себя этапы компрессии, шифрования и помехоустойчивого кодирования. Поэтому основная цель статьи заключается в рассмотрении основных вариантов защиты информации видеоинформационных ресурсов в инфокоммуникационных системах.

Процесс шифрования может быть реализован на разных этапах формирования обработки и передачи данных, а именно: до сжатия, во время сжатия, после сжатия.

В случае использования шифрования до сжатия (вариант 1) объем исходных данных, равный, после шифрования не изменяется. В процессе шифрования структура видеопотока разрушается – снижается потенциальное количество статистической, психовизуальной и структурной избыточности, вплоть до нулевого уровня. Это приводит к устранению меньшего количества избыточности. Следствием вышеуказанного является увеличение объема данных после их сжатия. Из-за увеличения объема сжатых шифрованных данных время, затраченное на передачу сжатых шифрованных данных, будет больше времени передачи исходных сжатых данных.

Время на обработку и передачу данных зависит от объема переданных данных, который увеличивается после сжатия шифрованных данных по сравнению с исходным объемом данных. Следовательно, время на передачу исходных сжатых данных будет меньше времени на передачу обработанных данных, которые включаю в себя процессы шифрования и сжатия.

Данная реализация обработки и передачи данных обладает такими положительными качествами как: не происходит увеличение объема шифрованных данных, высокая криптостойкость из-за возможности применения сложных алгоритмов шифрования. В то же время существенными недостатками являются: увеличение объема сжатых шифрованных данных из-за разрушения структуры видеоданных в результате применения алгоритмов шифрования перед сжатием.

Для того чтобы избавиться от проблемы, связанной с увеличением объема сжатых шифрованных данных в результате разрушения структуры видеопотока в процессе шифрования, предлагается рассмотреть иной вариант, который заключается в шифровании и передачи ранее сжатых данных (вариант 2). В результате применения алгоритмов сжатия, объем сжатых данных будет меньше исходных.

После шифрования объем данных не меняется, поэтому объем шифрованных сжатых данных будет равный объему сжатых исходных данных. В результате применения алгоритма шифрования, общее время на обработку и передачу данных будет больше времени на передачу исходных сжатых

данных. Положительным моментам в таком решении является уменьшение объема сжатых шифрованных данных, но при этом увеличивается время на обработку этих данных.

Рассмотрев вышеописанные варианты с применением шифрования до и после процесса сжатия, можно сделать вывод о том, что на общее время обработки и передачи зашифрованных видеоданных влияют: применяемые алгоритмы шифрования, от которых зависит скорость шифрования, вычислительные мощности оборудования, от которых зависит весь процесс обработки видеоданных, скорость канала передачи данных.

Поэтому к рассмотрению предлагается вариант, в котором данные шифруются в процессе их сжатия (селективное шифрование). Такая реализация (вариант 3) применяется в случаях обработки и передачи данных в системах реального времени (например, видеоконференцсвязь). Для такого варианта сжатие и шифрование выполняются для исходных данных по мере поступления их на обработку. В таком случае объем, обрабатываемых данных с применением селективного шифрования, будет меньше объема исходных данных из-за применения алгоритмов сжатия, но больше, чем объем сжатых исходных данных из-за внедрения алгоритмов шифрования. Также объем, обрабатываемых данных с применением селективного шифрования, будет меньше объема сжатых зашифрованных данных из-за разрушения структуры видеоданных в результате применения алгоритмов шифрования перед сжатием. А объем зашифрованных сжатых данных будет меньше, чем объем данных с применением селективного шифрования.

Из-за интеграции шифрования в процесс сжатия, время селективного шифрования будет меньше, чем время сжатия с последующим за ним шифрованием. Следовательно, весь процесс обработки передачи видеоданных будет происходить быстрее.

Время, затраченное, на селективное шифрование, будет меньше, чем время на шифрование с последующим за ним сжатием, из-за значительного увеличения объема данных в процессе сжатия шифрованных данных, что также делает весь процесс обработки передачи видеоданных быстрее, чем в первом варианте.

Рассмотрев все три варианта применения алгоритмов шифрования, можно сделать вывод о том, что селективный подход является оптимальным для шифрования и передачи видеоданных, а именно: время на обработку и передачу видеоданных с применением селективного шифрования затрачивается меньше, чем при шифровании до или после процедуры сжатия; объем данных с применением селективного шифрования будет меньше объема данных, которые сначала шифруются, а потом сжимаются (вариант 1), но больше, чем объема данных, которые сначала сжимаются, а потом шифруются (вариант 2).

Управление рисками информационной безопасности судовождения

УДК 004.056(043.2)
Геннадій Вильский
Николаевский политехнический институт, Украина, g_vilsky@mksat.net

Обеспечение безопасности судовождения ежегодно усложняется и обостряется многочисленными угрозами и рисками аварийных ситуаций и происшествий. Анализ материалов аварийных дел показывает конгруэнтность проблем рисков морских судов и их ошибочного маневрирования в стесненных условиях плавания, акваториях портов и каналов, вследствие потери времени ориентации. Признано, что гарантированные условия безаварийного управления судном состоят в достоверности, адекватности и конфиденциальности сообщаемых судну навигационно – информационных параметров обстановки на маршруте, способности судоводителя объективно воспринимать потоки сведений и сообщений необходимых для дальнейшего прогнозирования развития опасных ситуаций. Объективная оценка существующего положения невозможна без рассмотрения во взаимосвязи информативности и аварийности судов. Она подтверждает актуальность глубокого научного исследования судна, как объекта информационной безопасности, проведение которого возможно на основе серьёзной статистики морских происшествий и требует создания инструментальных средств нового поколения по управлению рисками информационной безопасности мореплавания в составе береговых систем управления движением судов (СУДС).

Анализ исследований предмета внимания и существующих трудностей в обеспечении надёжного управления рисками судовождения показывает их связь с разработкой специальных методик представления и моделирования потоков информации в навигационных системах управления движением судов. Несмотря на детерминированное состояние СУДС их работа отличается разнообразием, сложностью, применяемым оборудованием и характеризуется не способностью оказывать информационно - аналитические услуги судовождению с выполнением оценки опасностей и управлением рисками информационной безопасности.

Целью выполнения исследования является разработка и представление научных инноваций в управлении рисками информационной безопасности судовождения.

В данной работе за риски информационной безопасности судовождения приняты последствия от нарушения принципов формирования и передачи/приёма на морское судно данных, приведшие к бедственному состоянию экипажа, судна или груза. Методом экспертных оценок, концептуальным и дескриптивным моделированием идентифицированы возможные риски информационной безопасности движения судна: "Посадка на мель"; "Столкновение"; "Навал"; "Ледовый"; "Техногенный"; "Враждебное действие". Каждое состоявшееся рисковое событие отражается на состоянии мореходных качеств судна, приносит ущерб огромной величины. Морской практикой выявлены пять видов потоков сведений и сообщений параметры,

которых создают информационные опасности и угрозы судовождению. Факторы угроз исходят из предпосылок (неадекватность, недостаточность, несвоевременность поступающих данных), а их отражение проявляется в виде (потеря ориентации в обстановке на мостике судна, состояние и ошибки оператора, враждебные действия), приводящем к наступлению неблагоприятных рисковых событий. При плавании в открытом море и на внутренних водных путях существующая проблема образования рисков аварийности судов может решаться путём повышения качества формирования и циркуляции информационных потоков СУДС. В результате изучения процесса управления движением судов установлена низкая эффективность и недостаточная способность береговых информационных систем противодействовать проявлениям внешним и внутренним воздействиям на управление судами. Существующие возможности отображения реальной навигационной обстановки на водном пути, методы и модели оценки местоположения судна отражают неспособность представлять в динамике с высокой достоверностью по всему маршруту вероятностную картинную экспозицию приближающихся опасностей на водном пути. Стало актуальным утверждение о важности и первостепенности в модернизации существующих или построении специальных СУДС на основе разработанной Концепции гарантированной информационной безопасности судна. В этой связи, обеспечение судоводителя навигационным ресурсом с предупреждением об опасностях обстановки на маршруте имеет решающее значение для принятия решений по безопасному управлению судном.

Предложенные автором методика вероятностной оценки информационной безопасности движения судна, кластеризация судовых информационных потоков по приоритетам, кластер информационной безопасности движения судна, расчёт информационного пространства судовождения вероятностно - статистическими методами с применением теоремы Радона – Никодима, компъютерная модель информационного пространства судовождения обеспечили создание концепции компъютерной информационно-аналитической системы (КИАС) нового поколения для управления рисками информационной безопасности судовождения. Устранение ассиметричности навигационного поля, в созданной КИАС, обеспечено реализацией аналитической функции оценки опасностей на водном пути. Завершающей фазой новой функции системы становятся рекомендации по безопасному движению судна в условиях действия опасных факторов и угроз. Наряду с широко применяемыми устройствами передачи/приема и обработки данных, система отличается присутствием новых оригинальных технических решений в виде блока базовых моделей (ББМ) и блоков определения и анализа новых опасностей. Вероятностные модели, создаваемые в КИАС по мере необходимости для определенных акваторий, пополняют базу данных блока ББМ, повышают уровень автоматизации работы системы в управлении рисками информационной безопасности судовождения. Разработанные теоретические положения информационного обеспечения КИАС позволяют гарантировать достоверность передачи и приёма судовой информации.

Техническая комплектация КИАС отвечает вызовам и проявлениям глобализованной мировой экономики в отношении судоходства. Обеспечивается решение задач с судовыми информационными рисками в соответствии с правилом главы V – "Безопасность мореплавания" Международной конвенции "СОЛАС-74/88", резолюциями Международной морской организации А.857(20) "Руководство для служб движения судов" и Международной ассоциации маячных служб "Руководство для СРДС", нормами международного стандарта ISO/IEC 27005 "Управление рисками информационной безопасности".

Все теоретические положения и технические решения, заложенные в КИАС, повышают эффективность работы мостика судна за счёт функционирования инструментария управления рисками информационной безопасности судовождения, гарантируют сохранность жизни членам экипажей, судна, и перевозимых грузов.

Фактори економічної безпеки системи економіки авіатранспортного комплексу країни як складова інформаційної безпеки держави

УДК 004.056(043.2)

Андрій Міщенко
Національний авіаційний університет, Україна, vvk@zeos.net

Актуальність. Виникнення поняття «інформаційна безпека держави» для економіки України пов’язане з переходом саме «сталої» економічної системи з державною власністю на засоби виробництва та національну валюту (планової економіки соціалізму) до «вільної» ринкової економіки з приватною власністю на засоби виробництва та комерціалізацією національної валюти (економіки капіталізму).

Метою цієї доповіді є розгляд та аналіз факторів економічної безпеки системи економіки авіатранспортного комплексу країни як складової інформаційної безпеки держави.

Економіка авіатранспортного комплексу як складова інформаційної безпеки країни є одною з основних сфер діяльності суспільства по задоволенню його життєвих матеріальних потреб.

Функція розподілу верств авіаінфраструктури [2] за значенням *n* градацій доходу *f(x)* і чисельність робітників регіону *NS* пов’язані очевидним рівнянням:

$$NS = \int_{-\infty}^{+\infty} f(x)dx \approx \sum_{i=1}^{n} f(x_i)\,, \qquad (1.17)$$

Середньозважене значення річного доходу *1* особи (в умовних одиницях у.о.) для наявної функції густини розподілу *{f(x)/NS}* –

$$M[XS] = \int_{-\infty}^{+\infty} x \cdot \left(\frac{f(x)}{NS}\right) \cdot dx \approx \frac{1}{NS}\sum_{i=1}^{n} x_i \cdot f(x_i) = 578.00 \text{ тис.у.о.} \qquad (1.18)$$

Дисперсія функції густини розподілу –

$$D[XS] = \int_{-\infty}^{+\infty} (x - M[XS])^2 \cdot (\frac{f(x)}{NS})dx \approx \sum_{i=1}^{n} (x_i - M[XS])^2 \cdot f(x_i) = 129886 \quad (1.19)$$

і середньоквадратичне відхилення доходів від *M[XS]* –

$$\sigma[XS] = \sqrt{D[XS]} = 360.40 \text{ тис.у.о.} \quad (1.20)$$

Очевидно, сумарний загальний доход цілої галузі авіатранспортного комплексу –

$$DS = \int_{-\infty}^{+\infty} x \cdot f(x)dx = M[XS] \cdot NS = 7\ 237\ \ 294 \text{ тис.у.о.} \quad (1.21)$$

Якість розподілу доходів робітників галузі [3], як ступінь «густини» доходів навколо середньозваженого значення (критерій «усі рівно багаті»), оцінюється показником –

$$Q(XS) = 1 - \frac{\sigma[XS]}{M[XS]} = 1 - \frac{360.40}{578.00} = 0.376 \ .$$

У даному випадку цей показник, що відображає рівень соціальної справедливості економічної системи, низький через шкоду «експлуатації» меншістю робітників його більшості і його розшарування по рівню добробуту.

По-друге, об'єктивним економічним показником добробуту робітника є відносний, до поточної вартості «кошика споживача» (КС) на поточний період часу *c(τ)*, середній рівень його доходу *dτ (t)* для усіх вікових категорій –

$$r_i = d_i / c_i, \ \ i = \overline{1,7}$$

Наприклад, в якості періоду τ обирається сезон року (зима, весна, літо, осінь) і обчислюється рівень добробуту для усіх вікових категорій громадян регіону (табл.1.1).

Таблиця 1.1

Обчислення рівню добробуту робітників галузі

Вікова катего-рія	Вік (років)	Вартість КС на період τ (тис.у.о.)	Дохід за період τ (тис.у.о.)	Рівень добробуту
k_1	01-10	c_1=6	d_1=7	r_1=1.167
k_2	11-20	c_2=9	d_2=12	r_2=1.133
k_3	21-30	c_3=12	d_3=15	r_3=1.250
k_4	31-40	c_4=15	d_4=18	r_4=1.200
k_5	41-50	c_5=18	d_5=21	r_5=1.167
k_6	51-60	c_6=15	d_6=18	r_6=1.167
k_7	61-70	c_7=12	d_7=15	r_7=1.250
k_8	71 і більше	c_8=9	d_8=12	r_8=1.133

Таким чином, основною умовою економічної системи економіки авіатранспортного комплексу як складової безпеки країни на сучасному ринку є утримання його максимальної системної ефективності.

Захищений навчально-методичний комплекс дисципліни "Інформаційне забезпечення управлінської діяльності"

УДК 004.056.5(043.2)

Аліна Задерій, Артем Фузік
Національний авіаційний університет, Україна, alina_zaderiy@ukr.net, artem.fuzik@gmail.com

На сучасному етапі розвитку освіти дистанційне навчання розглядається як індивідуалізований процес передання та засвоєння знань, умінь, навичок і способів пізнавальної діяльності особистості, який відбувається за опосередкованої взаємодії віддалених один від одного учасників навчання у спеціалізованому середовищі, яке створене за допомогою використання сучасних психолого-педагогічних та інформаційно-комунікаційних технологій.

Навчально-методичний комплекс (НМК) визначає сукупність дидактичних і методичних матеріалів, спрямованих на реалізацію освітніх послуг певної науки або галузі знань. Актуальність даної роботи полягає у підготовці конкурентоспроможного фахівця з опанованим ним рівнем компетенції, згідно стандартів навчальних закладів. Мета роботи полягає у створенні НМК дисципліни "Інформаційне забезпечення управлінської діяльності", забезпеченні цілісного навчального процесу, який включає визначені "Положенням про організацію навчального процесу у вищих навчальних закладах" форми, методи і засоби навчання у ВНЗ.

Для досягнення поставленої мети необхідно вирішити наступні задачі: Провести аналіз характеристик існуючого сучасного навчально-методичного забезпечення; визначити основні компоненти НМК "Інформаційне забезпечення управлінської діяльності"; розробити НМК дисципліни "Інформаційне забезпечення управлінської діяльності" за методологією TRAINAIR. (Розробка лекційних та лабораторних занять, варіантів модульних контрольних робіт і тем домашньої роботи).

Новизна роботи полягає у автоматизації процесу навчання, за рахунок впровадження дистанційних форм навчання.

Цей комплекс складається з теоретичного матеріалу, лабораторних робіт, питання для модульного контролю та завдання до виконання індивідуальних завдань.

Навчально-методичний комплекс дисципліни "Інформаційне забезпечення управлінської діяльності" необхідний для самостійної роботи при очному і, особливо, дистанційному навчанні , тому що полегшує вивчення матеріалу за рахунок доступності до навчального ресурсу в мережі Інтернет. Також розроблено захист електронного ресурсу для запобігання несанкціонованому розповсюдженню інформації. Цей НМК може застосовуватись студентами та фахівцями з напрямку "Управління інформаційною безпекою " та суміжними напрямами.

Науковий керівник — к.т.н. Євгенія Іванченко

Захищений навчально-методичний комплекс дисципліни «Інформаційні технології організації бізнесу»

УДК 378.147:004:658.8(0432)
Вероніка Духно, Анна Корченко
Національний авіаційний університет, Україна, veronikaduhno@mail.ru, annakor@ukr.net

На сьогодні розроблені галузеві стандарти вищої освіти України галузі знань 1801 «Специфічні категорії» напряму підготовки 8.18010015 «Консолідована інформація», за якими були створені навчальні плани. На їх основі написані навчальні та робочі навчальні програми з дисципліни «Інформаційні технології організації бізнесу», але для неї немає відповідного навчально-методичного забезпечення (НМЗ), тому створення навчально-методичного комплексу (НМК) є актуальною задачею. Дана навчальна дисципліна є теоретичною основою сукупності знань та вмінь, що формують управлінський профіль фахівця в області інформаційно-аналітичної діяльності та технологій.

Мета роботи полягає у вдосконаленні НМЗ шляхом створення захищеного НМК дисципліни «Інформаційні технології організації бізнесу» за методологією TRAINAIR. Основним завданням роботи є проведення аналізу існуючого НМЗ та розробка НМК зазначеної дисципліни, який включає в свою структуру: лекційний матеріал, лабораторні заняття, теми домашніх робіт, варіанти тестових та модульних завдань.

Метою викладання дисципліни є розкриття сучасних наукових концепцій, понять, методів та інформаційних технологій управління, дослідження управлінських систем на прикладі сучасних інформаційного-аналітичних систем управління бізнесом в умовах взаємодії з динамічним навколишнім середовищем, а також процесів провадження інформаційно-аналітичних систем в управлінні. Головними завданням вивчення дисципліни є: оволодіння методами та технологіями використання інформаційних систем для автоматизації роботи бізнесу та формування спектру задач в управлінській діяльності, з урахуванням динамічних змін навколишнього середовища; дослідження алгоритмів прийняття управлінських рішень за допомогою інформаційно-аналітичних систем; дослідження типів інформаційних систем управління, ознак організації як інформаційного механізму, методів прийняття управлінських рішень та принципів побудови систем підтримки їх прийняття; оволодіння базовими методами та процесами управління економічною та управлінською інформацією.

Запропонований НМК дасть змогу студентам і фахівцям, які підвищують кваліфікацію пройти курс та здійснити самоконтроль знань дисципліни «Інформаційні технології організації бізнесу», а відповідний захист НМК дозволить уникнути його несанкціонованого копіювання та модифікації, що забезпечить вдосконалення набутих знань та вмінь відповідних фахівців напряму підготовки 8.18010015 «Консолідована інформація».

Науковий керівник — к.т.н. Анна Корченко

Система інтелектуального фаззінгу

УДК 004.056(043.2)
Марина Савчук, Юлія Коваленко
Національний авіаційний університет, Україна, maryna_savchuk@ukr.net, ivanchyk_81@mail.ru

Система, яка поєднує в собі характеристики різних фаззерів та наділена їхніми перевагами називається системою інтелектуального фаззінгу. Використання такої системи дає можливість комплексного пошуку вразливостей з допомогою фаззінгу. Фаззінг – це спосіб тестування додатків, в онові якого лежить передача деяких випадкових даних в об'єкт,що досліджується з метою виклику ситуації збою чи помилки. Якщо при роботі програми виникла помилка або виключна ситуація, то, можливо, в програмі присутня вразливість. Фаззінг – це процес передбачення, які типи програмних помилок можуть бути виявлені в продукті, які саме значення вводу викликають дані помилки. Дані передаються на вхід програмним інтерфейсам, що включають: файли, мережеві протоколи, API. Актуальним є пошук вразливих місць системи, оскільки дані місця дають можливість нанести системі ушкоджень. У комп'ютерній безпеці термін вразливість використовується для визначення недоліків в системі, що може призвести до порушення її цілісності і викликати неправильну роботу системи. Фаззінг визначає загальний підхід до виявлення вразливостей, проте за його допомогою можна визначити різні індивідуальні методи застосування загальної методології. Конкретної методології фаззінгу немає, але можна виділити наступні основні категорії: 1) завчасно підготовлені ситуації для тестування (розробка ситуацій для тестування починається з вивчення початого прикладу для визначення структурних даних та прийнятних значень для кожної з цих структур. Пізніше створюються пакети з жорстким кодом або файли, за допомогою яких досліджуються граничні умови чи вносяться помилки в програму.); 2) випадкові дані (принцип використання випадкових даних полягає у вкиданні псевдовипадкових даних в об'єкт і в очікуванні поведінки досліджуваного об'єкта); 3) мутаційне тестування протоколу вручну (при ручному тестуванні протоколу автоматичні фаззери не застосовуються. Фактично, дослідник сам являється фаззером, оскільки самостійно вводить невірні дані з метою виклику небажаної поведінки об'єкта); 4) мутаційне тестування або тестування методом «грубої сили» (цей метод являється одним із самих ранніх. Він майже не потребує попередніх дослідів. Для застосування даного методу потрібна тільки зміна даних і їх передача). Фаззінг має ряд переваг перед іншими методами тестування програмного забезпечення. Їх прикладами являються: легка автоматизація; викликає виконання більшості перевірок в додатку; знаходження багатьох помилок; великий об'єм тестування з різними варіаціями; знаходження багатьох проблем пов'язаних з ненадійністю (багато з них являються потенційними проблемами безпеки).

Система інтелектуального фаззінгу дає можливість комплексного рішення пошуку вразливостей. Порівняння таких систем дозволяє здійснити

обгрунтований вибір системи інтелектуального фаззінгу для розв'язання задач підвищення захищеності програмного забезпечення.

Програмна система управління активами підприємства

УДК 65.012.8:658.12(043.2)
Лідія Кутна, Світлана Казмірчук
Національний авіаційний університет, Україна, lidakutna@gmail.com, sv902@mail.ru

У зв'язку із стрімким розвитком інформаційних технологій і систем автоматизації, а також їх впровадження в процеси управління підприємством та забезпечення бізнес-процесів, зумовлюється значне збільшення кількості ризиків і потенційних загроз життєдіяльності компанії. Беручи до уваги те, що інформаційна безпека (ІБ) сьогодні – це 80% менеджменту та 20% технології, актуальність побудови ефективної системи менеджменту інформаційної безпеки (СМІБ) не викликає сумнівів. Одним з етапів впровадження системи згідно стандарту ISO 27001 є реалізація процесу управління активами підприємства, що забезпечує їх оцінювання та ідентифікацію.

Здійснивши аналіз міжнародних стандартів стосовно впровадження системи менеджменту ІБ та безпосередньо управління активами, таких як ISO 27001, ISO 55000, PAS 55 та SAE JA 1011, 1012, а також існуючих на ринку програмних продуктів було отримано результат, який показав, що на сьогоднішній день немає єдиного програмного рішення проблеми автоматизації обліку всіх можливих активів підприємства для здійснення управління ними шляхом оцінювання та ідентифікації. У зв'язку з цим актуальною є розробка програмного засобу, який дасть змогу здійснити підтримку процесу управління активами на підприємствах різного роду діяльності згідно вимог міжнародних стандартів.

Метою даної роботи є розробка програмної системи управління активами підприємства в основу якої покладено оцінювання та ідентифікацію всіх типів активів, що присутні на будь-якому підприємстві.

Для досягнення поставленої мети було досліджено наступне програмне забезпечення: IBM Maximo Asset Management, Infor10 EAM Asset Sustainability та Галактика ЕАМ, в їх основу покладено орієнтування на певну сферу діяльності або охоплення управління діяльністю підприємства в цілому, не концентруючи увагу виключно на управлінні активами. Так, програма IBM Maximo Asset Management не орієнтована конкретно на роботу з управління активами і намагається охопити всі рівні менеджменту підприємства, що не дає можливості сконцентруватись виключно на здійсненні обліку активів, забезпечення їх управління та належного функціонування в роботі підприємства, а це в свою чергу може привести до виникнення ризиків та загроз життєдіяльності організації. Infor10 EAM Asset Sustainability включає в себе профілактичне обслуговування активів в дискретному виробництві і компаніях харчового сектору, управління енерговитратами в целюлозно-паперовому секторі, облік ризиків в медицині, управління парком техніки в

транспортних компаніях, контроль лінійних активів в нафтогазовому секторі, моніторинг основних засобів і їх обслуговування в залежності від технічного стану в державних організаціях, але дана система не прилаштована до роботи з бізнес-процесами, що протікають на підприємствах пов'язаних з фінансами, наприклад, банківські установи. Галактика EAM зосереджена лише на управлінні виробничими активами, вона дозволяє реалізувати моніторинг технічного стану обладнання та на основі системи критеріїв визначати аварійні об'єкти, що вимагають обслуговування і ремонту.

Дослідивши важливість управління активами на підприємстві та взявши за основу існуюче програмне забезпечення, було розроблено автоматизовану систему оцінки та ідентифікації активів для забезпечення процесу управління ризиками з доступним та інтуїтивно зрозумілим інтерфейсом, що дозволяє користувачу без спеціалізованих навиків використовувати її у діяльності організації.

Розроблена система орієнтована виключно на управлінні активами, що дає змогу оцінити всі існуючі активи на підприємстві незалежно від сфери діяльності і включає в себе: 1) управління бізнес-процесами; 2) управління ресурсами; 3) управління обладнанням; 4) управління IT-активами; 5) управління фінансовими активами.

При створенні методики опису активів використовувався процесний підхід та модель «Plan-Do-Check-Act» (цикл Шухарта-Деминга), згідно якої реалізується безперервне поліпшення процесу інформаційної безпеки організації. Відповідно до даної методики створюється реєстр активів, тобто подається розгорнута таблиця в якій відображаються існуючі активи організації.

Під час опису активів використовуються такі атрибути: 1) назва активу; 2) рівні забезпечення; 3) максимальний час недоступності; 4) власник активу; 5) місце знаходження активу; 6) категорія активу.

Для здійснення оцінки активів використовується трьох рівнева шкала оцінки градації, що включає в себе низький, середній та високий рівні.

Також було проведено експериментальне дослідження системи, в ході виконання якого отримано звіт у вигляді готового реєстру, який видає детальний опис активів підприємства, що ранжуються за коефіцієнтом важливості.

Розроблена програмна система аналізу та оцінювання активів підприємства дозволяє, за рахунок системного підходу до ідентифікації усіх ресурсів та бізнес-процесів, які мають цінність для підприємства, підвищити ефективність управління активами, дає змогу, враховуючи підходи міжнародних стандартів, службі захисту інформації організації підвищити ефективність функціонування (швидкодія, точність, вартість) і може бути використана на підприємстві будь-якого типу, від медичних закладів до банківських установ.

Система оцінки фінансового збитку від інсайдерських атак

УДК 65.012.8(043.2)
Вадим Шишкін
Національний авіаційний університет, Україна, kievradnik@ukr.net

Аналіз нормативної бази України, демонструє відсутність законодавчих актів, які регулювали б операції з інсайдерською інформацією. Проаналізовано методи захисту від інсайдерських загроз, де можна виділити 5 класів рішень, а саме захист від витоків (Anti-Leakage Software), кошти внутрішнього контролю (Internal Controls), системи сильної аутентифікації (3A: аутентифікація, авторизація, адміністрування), запобігання нецільового використання поштових ресурсів та Інтернету, архівація корпоративної кореспонденції.

Актуальність проблеми інсайдерства полягає в тому, що багато українських замовників ставлять проблему витоку інформації на перше місце. Першою в рейтингу стоїть проблема інсайдерства, тобто втрати компаній від дій інсайдерів значно більше, ніж від будь-чого іншого. На даний момент ми спостерігаємо в Україні значний інтерес клієнтів до тих продуктів, які орієнтовані на захист від внутрішніх загроз.

Головною метою є розробка системи оцінки фінансового збитку від інсайдерських загроз. Тобто розробка системи, що включає в себе декілька методик оцінки збитку від витоку конфіденційних даних.

Проаналізовано, що 82% загроз реалізується власними співробітниками фірми або при їх прямій чи опосередкованій участі, 17% загроз реалізується ззовні підприємства і всього 1% загроз реалізується випадково.

Розроблена система оцінки фінансового збитку від інсайдерських загроз, що є сукупністю декількох методик, які за допомогою математичних моделей можливого збитку від витоку конфіденційної інформації в інформаційних системах, а також моделі «обізнаність-ефективність», оцінка збитків внаслідок зниження ефективності захисту дає можливість кількісної оцінки величини фінансового збитку, який завдається діяльністю інсайдерів та може ґрунтуватися на двох засобах. Перший застосовується у випадку, коли об'єктів захисту може бути декілька та полягає у визначенні додаткових матеріальних витрат, необхідних для відновлення втраченої ефективності об'єкта шляхом застосування додаткової кількості об'єктів захисту. Другий спосіб оцінки збитку застосовуємо для одиничних об'єктів захисту, є і ґрунтується на оцінці грошових витрат на створення захисту з необхідною проектною ефективністю.

Негативні наслідки від даної загрози можна пояснити нездатністю сучасних рішень з нею боротися. Засоби захисту від несанкціонованого доступу тут є практично марними, оскільки в якості основного джерела загрози виступає «інсайдер» - користувач інформаційної системи, що має цілком легальний доступ до конфіденційної інформації і застосовує весь арсенал доступних йому засобів для того, щоб використовувати конфіденційну інформацію в своїх інтересах. Тому можливість кількісної оцінки фінансового збитку від цієї категорії загроз, дає нам уявну картину, наскільки інформація є цінною та які затрати понесе компанія, у разі втрати цієї інформації.

Науковий керівник – к.т.н. Анна Корченко

Програмний модуль захищеного інтерактивного інформаційного обміну

УДК 004.056.55(043.2)
Анастасія Дімнич
Національний авіаційний університет, Україна, nastikd92@mail.ru

В сучасному інформаційному світі безперервно збільшуються обсяги інформації з обмеженим доступом, тому гостро постає питання захищеного обміну такою інформацією в інтерактивному режимі. У випадку передачі інформації в мережі у вигляді повідомлень, ефективним є криптографічний захист даних, що передаються. Разом із розвитком інформаційних технологій зростає кількість інформаційних ризиків та стають легшими реалізації атак. Кількість методів криптографічного захисту інформації є досить великою, проте розробка нових та вдосконалення вже існуючих не втрачає своєї актуальності.

Метою роботи є підвищення ефективності захищеного інтерактивного обміну великих об'ємів даних шляхом розробки швидкісного програмного модуля криптографічної обробки даних та її подальшої передачі в мережі.

Було розглянуто основні криптографічні алгоритми, їх переваги та недоліки, а також проаналізовано сучасні вимоги до алгоритмів шифрування, котрі формуються на конкурсах вибору стандартів шифрування, зокрема AES та NESSIE. Спираючись на виявлені недоліки алгоритмів, необхідність їх вдосконалення та на сучасні програмні модулі захищеного інформаційного обміну, обрано для вдосконалення та використання у роботі, алгоритм Serpent. Даний алгоритм є симетричним блоковим алгоритм у вигляді SP-мережі.

Отримано подальший розвиток методу криптографічного захисту інформації, а також алгоритму шифрування даних з метою передачі в інтерактивному режимі. У роботі реалізований програмний модуль інтерактивного інформаційного обміну за новим алгоритмом. Довжина блоку вхідних даних становить 256 біт, а число раундів – 16. Раунди алгоритму повторюються таким чином: раунди під непарними номерами виконують функції першого раунду, під парними номерами – функції другого раунду. Раунди відрізняються операцією додавання ключів раунду. Над блоками даних виконується нелінійна заміна байтів, використовуючи таблицю замін, котра будується шляхом отримання зворотного числа в полі Галуа GF(28) та виконання до кожного байту певної операції. Також виконується процедура, при якій байти змішуються, використовуючи зворотну лінійну трансформацію. Застосування цієї операції забезпечує розсіювання байтів зашифрованих даних.

Було досліджено статистичні характеристики криптостійкості розробленого симетричного алгоритму за допомогою методики NIST STS. Розроблений програмний модуль захищеного інтерактивного обміну дав змогу підвищити швидкість шифрування даних на 15% у порівнянні з алгоритмом ДСТУ ГОСТ 28147:2009. Підвищення швидкості криптографічної обробки даних дозволило покращити умови інтерактивного обміну даними шляхом зменшення часу, необхідного для передачі інформації.

Науковий керівник — д.т.н. Володимир Хорошко

Захищена програмна система тестування користувачів для дистанційної форми навчання

УДК 044.056(043.2)
Анастасія Сєрікова
Національний авіаційний університет, Україна, anastinserikova@mail.ru

Провідні українські ВНЗ активно впроваджують дистанційні форми навчання з контролем знань та вмінь студентів за допомогою систем тестування. Головною задачею таких систем є отримання результату опитування, або оцінювання користувача. Цей результат повинен бути об’єктивний та достовірний, бо інакше існування такої системи і самого опитування не має ніякого сенсу. Об'єктивність отриманих за допомогою системи тестування результатів залежить від таких факторів: професійно складених тестових завдань та якості системи тестування, яка використовується. А от достовірність залежить від якості розробленої системи захисту. Тому створення системи тестування користувачів, що забезпечить не тільки об’єктивний, а ще й достовірний результат є актуальним завданням на сьогодні.

Метою роботи є розробка системи тестування користувачів із процедурою посиленого захисту від стороннього втручання, яка буде виконана за технологією трирівневих баз даних. Новизною роботи є впровадження нової процедури захисту, за рахунок якої вся обробка даних виноситься в інший файл, який знаходиться на сервері, що виключає можливість атаки типу SQL injection.

Запропонована модель захищеної системи тестування виконана за технологією трирівневих баз даних та працює наступним чином. При авторизації користувач вводить свій логии й пароль, ці дані звіряються з наявними в базі даних. Якщо авторизація пройшла успішно, то користувач переходи на сторінку тестування, при цьому програмно генерується унікальне значення яке міститься з однієї сторони в змінні сервера, а з іншого боку - в cookies браузера, цим ми захищаємо себе від подальшого XSS нападу. Потім на сторінці тестування користувач проходить тест, при цьому кожне наступне питання завантажується з окремого модуля. В цьому модулі відбувається порівняння даних з масиву змінних сервера і даних з cookies у випадку їх збігу модуль виконує всі покладені на нього функції: проводить з’єднання з базою даних, а отримані дані перетворить в XML структуру, що оброблюється JavaScript сценарієм на сторінці користувача.

Всі дані, що вводяться користувачем, проходять кілька фільтрів, крім того користувач не має прямого звертання до БД що виключає можливість атаки типу SQL injection. Даний спосіб захисту є досить надійним, а розроблена система тестування має ряд переваг перед існуючими програмами.

Дана система тестування може бути адаптована під різні потреби. Наприклад може бути впроваджена в системі дистанційного навчання, або на сайті будь-якої організації в якості системи опитування користувачів.

Науковий керівник – к.т.н. Євгенія Іванченко

Програмний модуль вибору систем протидії кібератакам

УДК 004.056.5
Надія Славченко
Національний авіаційний університет, Україна, nadia-slavchenko@mail.ru

Мета роботи виражається в рекомендаціях для полегшення здійснення вибору системи протидії кібератакам на основі ключових характеристик даних систем.

Актуальність. В даному випадку ключовою потребою є необхідність в організації стійкої системи захисту на всіх рівнях функціонування. Проте доволі часто виникають труднощі в оптимальному виборі необхідного засобу захисту. Актуальним є створення та використання програмного модуля, що допоможе користувачам значно полегшити процес вибору необхідної системи, насамперед, актуальних саме відносно даної ситуації засобів та методів.

Для вирішення цієї проблеми існують різноманітні методики вибору та системи підтримки прийняття рішень. Проаналізувавши такі методики можемо визначити, що основними їх недоліками є те, що вони характеризують системи захисту лише за декількома ознаками, тому рекомендації для вибору будуть не повними та, можливо, не досить точними для комплексного захисту.

Основна мета даного продукту полягає у об'єднанні декількох програмних засобів в межах одного інтерфейсу для полегшення прийняття рішення щодо використання певного програмного додатку, що відповідно впливає на рівень захищеності всієї системи.

Для даного програмного модуля відповідно першим критерієм підбору має бути ціна. Відносно до ціни виконується аналіз засобів захисту за певними якостям. Наступним кроком є вибір напрямку діяльності, тобто засіб мережевого чи системного типу збору інформації. Наступні критерії, тобто частота перевірок, спосіб аналізу, наявність аудиту, поведінка після виявлення, метод виявлення вказують на степінь ефективності та рівень захисту засобу організації безпечного функціонування інформаційного середовища. Якщо не має потреби у максимальному захисті, то аудит та спосіб аналізу не є ключовими аспектами вибору системи захисту. Відповідно метод виявлення, частота перевірок та поведінка після виявлення визначають ступінь надійності вибраного засобу.

Отже найефективнішим є захист, що базується на постійній активності, інтелектуальному методі виявлення та активному виконанні операцій протидії після виявлення. Отже відбір необхідно робити спираючись в першу чергу на потрібний рівень захисту та ціну програмного продукту.

Висновок. В даний момент більшість програмних додатків спрямовані на вирішення комплексних проблем захисту інформаційного середовища від кібератак різних типів. Але доволі часто такі методи не дають необхідного результату. Саме по цій причині потрібно формувати системи захисту на базі ПЗ одно-направленого, проте високоспеціалізованого напрямку протидії. Комбінування даного роду додатків дасть можливість реалізувати ефективний захист у всіх напрямках виникнення загроз.

Науковий керівник — д.т.н. Володимир Хорошко

Система захисту цілісності даних на основі хеш-кодів

УДК 004.056.5 (043.2)
Денис Москаєв
Національний авіаційний університет, Україна, estoner@mail.ru

Загрози цілісності даних займають значне місце в інформаційній безпеці. Своєчасне виявлення порушення цілісності цифрових даних дає змогу помітити дії інсайдера, незважаючи на те, навмисні вони чи випадкові, та дає можливість уникнути серйозних проблем і помітити шкоду нанесену зловмисником. Тому створення програмних засобів, що будуть своєчасно виявляти порушення цілісності даних є дуже актуальним в умовах сучасного ринку.

Метою роботи є створення програмної системи своєчасного виявлення порушення цілісності даних, яка поєднує у собі два підходи – моніторинг даних та перевірка хеш-кодів. Новизна роботи полягає у створенні методу для забезпечення цілісності інформації, що дасть змогу додатково своєчасно сповіщати щодо порушення її цілісності.

Аналіз ринку програмних засобів, що здатні перевіряти або контролювати цілісність інформації показав, що одна половина програмних засобів основною функцією має моніторинг каталогів та файлів, реєстру, системи, а друга половина програмних засобів основною функцію має підрахування та порівняння хеш-кодів, але лише за запитом користувача. Отже було прийнято рішення створити програмну систему, що буде поєднувати ці основні дві функції. Для вирішення поставленої задачі був розроблений власний метод, який поєднав у собі функції моніторингу файлів та папок, а також підрахунку і порівняння контрольних сум.

На основі запропонованого методу була створена програмна система, особливістю якої є те, що вона поєднує у собі два підходи – моніторинг каталогів та файлів, та підрахунок і порівняння хеш-кодів, що відповідає за перевірку цілісності файлів та відбувається за ініціативою програми, а не користувача. Таким чином забезпечується постійна перевірка цілісності файлі. Внаслідок чого стає можливим своєчасне виявлення порушення цілісності даних та застосування певних мір по запобіганню негативним наслідкам.

Тестування створеної системи показало, що створений програмний засіб працює коректно і виконує усі необхідні функції. Для кращого розуміння переваг створеної програмної системи було зроблено її порівняння з існуючими програмними рішеннями за декількома критеріями (порівняння та підрахунок хеш, моніторинг каталогів та файлів, сповіщення про порушення та ін). Особливістю програми є те, що вона може працювати постійно в активному режимі і відслідковувати усі зміни хеш-кодів самостійно, а не тільки за запитом користувача. В даній розробці це забезпечується за допомогою функції реагування за доступом до файлу. Тобто програмна система порівнює хеш-коди тоді, коли визначає, що було звернення до файлу, без перевантаження системи в цілому. Таким чином відбувається своєчасне виявлення порушення цілісності даних.

Науковий керівник — к.т.н. Микола Тимошенко

Інтелектуалізована інформаційно-аналітична система для підтримки прийняття рішень у сфері захисту інформації. База даних

УДК 004.651.4:004.056.5 (043.2)

Яна Веремієнко
Національний авіаційний університет, Україна, ver_yana@ukr.net

При прийнятті рішень на різних рівнях сучасних систем потрібні обробка та аналіз даних великого обсягу. Для вирішення таких завдань використовуються системи підтримки прийняття рішень, сфера застосування яких практично необмежена – в тому числі і захист інформації. На сьогоднішній день перед експертом при прийнятті управлінських рішень у сфері захисту інформації постає завдання оперувати великими обсягами несистематизованої нормативно-правової документації, що негативно відображається на результатах та призводить до значних часових витрат. Тому, вибір критеріїв систематизації нормативної документації та розробка на їх основі бази даних інформаційно-аналітичної системи для підтримки прийняття рішень у сфері захисту інформації є актуальною задачею.

Мета роботи полягає у розробці критеріїв систематизації нормативної документації для бази даних інформаційно-аналітичної системи для підтримки прийняття рішень у сфері захисту інформації.

Для досягнення поставленої мети було вирішено наступні задачі: досліджено існуючі підходи до систематизації баз даних нормативної документації; розроблено базу даних інформаційно-аналітичної системи для підтримки прийняття рішень у сфері захисту інформації на основі вибраних критеріїв класифікації; досліджено розроблену базу даних на предмет коректності систематизації нормативної документації у сфері захисту інформації.

Існують такі відомі інформаційно-довідкові системи правового характеру: веб-портал «Урядовий портал», Головний правовий портал України «ЛІГА:ЗАКОН», веб-портал Верховної Ради України та Фонд нормативних документів Державної служби спеціального зв'язку та захисту інформації, які мають ряд недоліків: відсутність допомоги при прийнятті рішень, не багато-критеріальна галузева класифікація, низька ступінь інформативності та ін.

Розроблена база даних структурована за категоріями практичних завдань, що виникають у сфері захисту інформації, містить критерії систематизації нормативної документації та є підґрунтям для побудови інтелектуалізованої інформаційно-аналітичної системи для підтримки прийняття рішень. База даних призначена для зберігання фактів або гіпотез, які є результатом спілкування системи із зовнішнім середовищем, в якості якого зазвичай виступає користувач, що веде діалог з експертною системою.

В результаті запропоновано нову модель бази даних системи прийняття рішення на основі вибраних критеріїв систематизації нормативної бази у сфері захисту інформації, в якій роль користувача зведена до мінімуму.

Науковий керівник — к.т.н. Олексій Гавриленко

Інтелектуалізована інформаційно-аналітична система для підтримки прийняття рішень у сфері захисту інформації. Модуль обробки

УДК 004.047:004.056.5 (043.2)
Дмитро Демченко
Національний авіаційний університет, Україна, d1m-dem@rambler.ru

На сьогоднішній день, коли процес автоматизації різних видів діяльності прийшов практично на кожне сучасне підприємство, обчислювальні системи та комп'ютерні мережі дозволяють накопичувати великі масиви даних. Такий обсяг інформації, з одного боку, дозволяє виконувати більш точні розрахунки і робити докладний аналіз, з іншого - перетворює пошук необхідних рішень на складне завдання. Трапляються випадки, коли фахівці не можуть оперативно прийняти чітке рішення практичних задач у сфері захисту інформації, оскільки змушені оперувати великим обсягом даних, що значно уповільнює процес та спричиняє розумові навантаження. Виникає необхідність спростити завдання пошуку рішення в слабо формалізованих областях, тому розробка модулю обробки даних інформаційно-аналітичної системи для підтримки прийняття рішень у сфері захисту інформації є актуальною задачею.

Метою роботи є удосконалення інтелектуалізованої інформаційно-аналітичної системи для підтримки прийняття рішень у сфері захисту інформації модулем обробки даних на основі заданих критеріїв класифікації нормативної документації.

Для досягнення поставленої мети було виконано такі задачі: проведено аналіз існуючих модулів обробки нормативної документації та методів аналізу даних в системах підтримки прийняття рішень; на основі методу нечіткої логіки розроблено алгоритм та програмний додаток, що дозволяє в режимі діалогу прийняти рішення у сфері захисту інформації; проведено експериментальне дослідження розробленого модулю обробки.

В ході аналізу модулів обробки даних існуючих інформаційно-аналітичних систем, що оперують нормативною документацією, було виявлено, що вони реалізують пошукові методи, але жоден з них не передбачає невизначених дій користувача.

Систему підтримки прийняття рішень у сфері захисту інформації удосконалено модулем обробки даних, який взаємодіє з базою даних й інтерфейсом користувача. Модуль обробки реалізований на основі методу нечіткої логіки, який забезпечує діалогову взаємодію системи та кінцевого користувача, без якого система в принципі не може функціонувати. У процесі діалогу з користувачем, модуль обробки системи прийняття рішень оперативно порівнює можливі шляхи вирішення задачі на підставі закладених критеріїв та дозволяє користувачеві отримати відповіді на нечітко сформульовані питання. В результаті проведеної роботи було удосконалено систему підтримки прийняття рішень у сфері захисту інформації модулем обробки на основі аналізу нечітких даних, результатом роботи якого є ранжування та рейтинги аналізованих об'єктів, що дає можливість отримати сформований звіт з безпосередньою участю користувача.

Науковий керівник — к.т.н. Олексій Гавриленко

Система тестування сайту на проникнення

УДК 004.056(043.2)
Ольга Вовк, Кирило Ануфрієнко
Національний авіаційний університет, Україна, olya_vovk@list.ru, cyril@xakep.ru

Аудит безпеки сайту на наявність вразливостей сайту - є потужним інструментом для забезпечення інформаційної безпеки ресурсу.

Веб-застосунок є дуже важливим активом, незалежно від того, які функції він виконує на підприємстві. Ресурс повинен стабільно і безперебійно працювати. Забезпечити дані умови можливо тільки приділяючи належну увагу безпеці ресурсу, а саме такій процедурі, як аудит безпеки сайту.

Система тестування сайту на проникнення – це комплекс заходів з виявлення помилок та вразливостей сайту, скориставшись якими зловмисники можуть атакувати і зламати сайт.

Існує безліч тлумачень терміну «тестування на проникнення», але більшість з них засновані на одному з двох варіантів: мається на увазі або імітація дій реального зловмисника з реалізації несанкціонованого проникнення в інформаційну систему, що відповідає значенню терміна «penetration testing» на західному ринку послуг безпеки, або інструментальний аналіз вразливостей і оцінка критичності знайдених вразливостей для бізнесу, що в англомовному середовищі більше відоме як «security assessment».

Метою роботи є створення системи тестування на проникнення яка дає можливість визначити поточний рівень захищеності сайту.

Сценарій проведення тестування на проникнення включає наступні кроки: 1) Планування тесту; 2) Збір інформації; 3) Пошук вразливостей; 4) Проникнення в системи; 5) Написання та надання звіту; 6) Очищення систем від наслідків тесту.

Існують такі підходи до проведення тесту: 1) White box (білий ящик) – виконавець має доступ до систем і своєму розпорядженні повну інформацію про них; 2) Black Box (чорний ящик) – імітує групу хакерів, які мають тільки назву компанії і практично нульові відомості про цільову систему; 3) Grey Box (сірий ящик) – передбачає імітацію хакерів, що володіють інформацією частково.

Існує досить багато різних методологій по проведенню тестування на проникнення, найбільш корисними серед яких є Information Systems Security Assessment Framework (ISSAF), NIST 800-42 Guideline on Network Security Testing, Open Source Security Testing Methodology Manual (OSSTMM), Open Web Application Security Project (OWASP), Wireless Penetration Testing Framework. Найкращою методологією для тестування сайту є OWASP, оскільки він створений для забезпечення безпеки веб-застосунків.

В результаті нами створюється звіт, який містить детальний опис проведених робіт, всі виявлені вразливості системи та способи їх реалізації. Також звіт містить рекомендації щодо усунення знайдених вразливостей.

Тест на проникнення дозволяє відокремити критичні проблеми безпеки, що вимагають безпосередньої уваги, від тих, які становлять меншу загрозу.

Науковий керівник — к.пед.н. Юлія Коваленко

Модуль захисту ресурсів інформаційних систем від прихованого сканування

УДК 004.056(043.2)

Мирослав Савченков
Національний авіаційний університет, Україна,
miroslav.savchenkov@gmail.com

Проблема захисту ресурсів інформаційних систем від прихованого сканування виникла через те, що сучасні засоби захисту, які засновані в цілому на архівації, шифруванні, а також використанні самогенерованих кодів, з часом старіють і зловмисникам стає простіше оминати такий захист. Актуальність даної роботи полягає в необхідності захищати комерційні версії програмного забезпечення, яке використовується в інформаційних системах, від прихованого сканування його коду, адже це може призвести до економічних збитків. Метою даної роботи є створення модуля захисту ресурсів інформаційних систем від прихованого скасування. Новизною є застосування нових методів захисту, що дасть змогу покращити захищеність комерційних версій програмного забезпечення від скритого сканування коду.

В роботі було проведено класифікацію атак на програмне забезпечення, де атаки класифікувалися за такими основними параметрами як: взаємодія з політикою безпеки; дистанційність; зовнішній прояв; автоматизація; ініціалізаційна умова; наявність зворотного зв'язку; порушення характеристик безпеки; реляційна ознака; ступінь складності; а також тип базового ресурсу.

Було досліджено основні методи захисту ресурсів інформаційних систем, такі як: використання ліцензійної мітки; створення захищеного середовища виконання; перевірка цілісності програмного коду; парольний захист; винесення критичного програмного коду в окремий захищений модуль; прив'язка програмного забезпечення до унікальних ознак комп'ютерної системи; пакування та шифрування; використання програмно-апаратних засобів захисту ПЗ з електронними ключами; обфускація. Модуль захисту програмного забезпечення реалізовано на основі блокового поточного шифру Blowfish з доданою модифікацією та використанням обфускації. Використання даного модуля унеможливить здійснення прихованого сканування завдяки перекриванню всіх можливих слабких місць, тобто взявши будь-який виконуючий файл, котрий має бути захищений, ми маємо змогу його закодувати і додати обфускацію. Під час запуску виконуючого файлу він буде розпаковуватися в дапм пам'яті з додаванням обфускації, що унеможливить витягування інформації з дампа пам'яті, і лише після цього запуститься. Виконавши експериментальні дослідження необхідно виділити наступні позитивні сторони: обфускатор робить дизасембльований код важким для вивчення, перетворюючи IsLicensed() в x(); обфускатор конвертує код в native, роблячи непотрібним дизассемблінг; використання шифрування унеможливлює скрите сканування коду. Практична цінність розробленого модуля полягає в можливості його практичного застосування для захисту програмного забезпечення від прихованого сканування.

Науковий керівник — к.т.н. Микола Тимошенко

Модуль захисту конфіденційних даних на підприємстві філії «НИССАЦЕНТРУМ»

УДК 004.056.55
Антон Тарасенко
Національний авіаційний університет, Україна, tarasenko.antin@gmail.com

На даний момент існує багато алгоритмів шифрування різної складності та швидкості. Також існує і багато програм, основною функцією яких являється шифрування даних. Проаналізувавши існуючі на сьогодні програмні продукти було зроблено висновок, що всі вони дуже вузько направлені і не можуть бути модифіковані, оскільки продаються лише у відкомпільованому вигляді, отже удосконалення методів і засобів для захисту даних є актуальною задачею.

Метою роботи є розробка та реалізація модуля захисту конфіденційних даних з великою швидкістю та змінними параметрами шифрування. Новизно є розробка власної ефективної та гнучкої програмної реалізації з більш високою швидкістю шифрування для підприємства філії «НИССАЦЕНТРУМ», за рахунок використання бібліотек сучасник мов програмування.

Для вибору алгоритму шифрування, котрий ляже в основу шифрувального модуля було проаналізовано і порівняно симетричні криптоалгоритми, а саме DES, ДСТУ 28147:2009, Blowfish, RC5, IDEA. В результаті досліджень серед решти алгоритмів було виділено RC5 за рядом переваг: проста структура алгоритму; висока швидкість шифрування; структура алгоритму дуже гнучка до змін; процедури шифрування і розшифрування по алгоритму RC5 практично ідентичні.

Отже алгоритм шифрування RC5 має значні переваги, які роблять його програмну реалізацію ефективною з погляду використання обчислювальних потужностей процесора і пам'яті. На відміну від аналогічних алгоритмів низькі вимоги до апаратних ресурсів та змінні параметри алгоритму дають змогу легко адаптувати алгоритм RC5 до змін у вимогах безпеки програмного комплексу, що робить цей алгоритм оптимальним для використання як засобу забезпечення конфіденційності розроблюваного модуля захисту.

В роботі розроблено алгоритм та програмну реалізацію швидкодіючого модуля забезпечення конфіденційності інформаційних ресурсів зі змінними параметрами шифрування з використанням програмної бібліотеки для мови Delphi. Реалізовано основні процедури: шифрування та дешифрування даних, і окремо другорядні процедури: ініціалізація ключа, розрахунок підключів. Така структура програмного модуля дозволить використовувати окремі його елементи у різних місцях розроблюваного програмного продукту.

Під час тестування модуля шифрування було визначено параметри криптостійкості та швидкості шифрування залежно від довжини ключа, тобто 128, 192, 256 біт (відповідно 4,6 мбайт/с, 5,0 мбайт/с, 5,8 мбайт/с).

Науковий керівник — к.т.н. Євгенія Іванченко

Система підтримки прийняття рішень в галузі інформаційної безпеки

УДК 004.891:005.53(043.2)
Юлія Бойко, Максим Іваненко
Національний авіаційний університет, Україна, i_max@i.ua

На сьогоднішній день досить актуальним є питання вибору, що і не оминуло галузь інформаційної безпеки. Ця галузь як і інші потребує доцільного, та якісного прийняття рішень. Це розуміють керівники підприємств та організацій і керівники держав. Природно, що чим вище рівень управління, тим більш вагомими та значущим є відповідне рішення. Проте й кількість факторів, які необхідно враховувати, у процесі прийняття рішень, значно більша. У зв'язку з цим виникає нагальна потреба в спеціалізованих засобах підтримки прийняття рішень. Насамперед мова йде про комп'ютерну підтримку діяльності керівників різного рівня. Вирішувати це завдання покликані комп'ютерні системи підтримки прийняття рішень (СППР).

Метою роботи є розробка системи підтримки прийняття рішень в галузі інформаційної безпеки з попередньою оцінкою компетентності особи, що приймає рішення (ОПР). Новизною роботи є те, що вперше запропоновано СППР яка поєднує в собі кількісні та якісні методи прийняття рішень, а також дає можливість перевірки компетентності ОПР, та дозволяє підвищити якість прийнятих рішень, за рахунок відсіювання некомпетентних осіб, які беруть участь у процесі прийняття рішень.

Аналіз існуючих СППР показав, що не всі вони можуть бути застосовані для вирішення задач в галузі інформаційної безпеки оскільки засновані або на статистичних методах, або на експертних методах підтримки прийняття рішень, що не завжди дає змогу знайти оптимальне рішення. Тому пропонується в одній системі поєднати статистичні та експертні методи ППР. Спираючись на виявлені недоліки методів, необхідність їх вдосконалення, обрано для використання у роботі такі статистичні методи ППР: частотні розподіли, групові середні, таблиці перерізів, парна регресія, та експертний метод – метод аналізу ієрархії.

Розроблена комп’ютерна система підтримки прийняття рішень складається з бази даних, модуля порівняння та модуля оцінки ОПР. Бази даних є основою системи, до неї заносяться ОПР альтернативи і критерії. Обрахунки проводяться в модулі порівняння на основі вищезазначених методів відповідно до поставленої задачі, вибір методу здійснюється ОПР. Модуль оцінки компетентності експертів дозволяє провести оцінку статистичним методом ранжування оцінюваних величин, евристичним методом самооцінки або експериментальним методом на основі запропонованого тестування.

Порівняння розробленої СППР з існуючими аналогами показало її переваги за рахунок попередньої оцінки компетентності ОПР, що дозволяє підвищити якість прийнятих рішень, за рахунок відсіювання некомпетентних осіб, які беруть участь у процесі прийняття рішень. А поєднання методів різних груп дозволяє приймати оптимальні рішення будь-якої складності.

Науковий керівник — к.т.н. Микола Тимошенко

Система поиска радиозакладных устройств

УДК 621.396.969.3: 65.012.8(043.2)
Сердар Тойчиев
Национальный авиационный университет, Украина, serdar_0112@mail.ru

В современном мире все большее значение приобретает защита информации, все больше и больше людей осознают важность безопасности информации. Одним из распространенных средств нелегального добывания информации в настоящее время является использование т.н. закладних устройств (жучков).Устанавливаемые скрутно в местах, где постоянно циркулирует конфиденциальная информация, они снимают информацию из аккустического канала утечки информации и передают по электромагнитному (или по другим: электрическому,оптическому и пр.) каналу.

Целью данной работы является улучшение технических характеристик аппаратуры поиска закладних устройств,а именно решение поставленного задания с помощью нелинейных локаторов.

На основании поставленной цели решаются следующие цели: анализ методов устройств обнаружения закладных устройств;анализ сравнительных характеристик нелинейных локаторов и их основных характеристик и принципов работы.

Нелинейные локаторы способны обнаруживать диктофоны на значительно больших расстояниях, чем металлодетекторы, и в принципе могут использоваться для контроля за проносом устройств звукозаписи на входах в помещения. Однако при этом возникает такие проблемы, как уровень безопасного излучения, идентификация отклика, наличие мертвых зон, совместимость с окружающими системами и электронной техникой.

Конструктивно устройство может быть выполнено, например, в виде классической рамки (аналог рамки металлодетектора) или установлено непосредственно в дверной проем кабинета. Задача обнаружения электронных изделий (в нашем случае – диктофонов) в режиме <рамка> требует определения двух основных критериев, предъявляемых к нелинейным локаторам:парамеиры передатчика локатора; параметры приемника локатора. Эти два параметра влияют еще на два важнейших эксплуатационных критерия: обнаружительная характеристика системы; безопасность использования нелинейного локатора для персонала в течение длительного времени. Особенность заключается в том, что эти два критерия являются антагонистическими. Цель пользователя системы-обнаружить все, имеющее отношение к радиоэлектронным устройствам, а это определяется обнаружительной характеристикой.

В целом, НЛ является эффективным средством раннего обнаружения аппаратуры звукозаписи, которое можно отнести к системам ограниченного доступа или к системам стационарного контроля.

Современные виды НЛ включают в себя достаточно много новых инженерных решений, которые делают поиск более точным и эффективным.

Научный руководитель — д.т.н. Владимир Хорошко

Комбінована система підтримки прийняття рішень у сфері інформаційної безпеки

УДК 004.891:005.53(043.2)
Юлия Бойко, Сергей Ноговський
Національний авіаційний університет, Україна, Lemon_helll@bigmir.net

На сьогоднішній день системи підтримки прийняття рішення (СППР) широко використовуються в різних сферах управління, в тому числі і в сфері управління інформаційною безпекою. Задачі інформаційної безпеки багатогранні і тому потребують не тільки формалізованих, а й неформалізованих методів вирішення. Тому створення СППР яка дає змогу обробляти інформацію в залежності від потреби особи, що приймає рішення є актуальним завданням.

Метою роботи є розробка комбінованої системи підтримки прийняття рішень на основі статистичних та експертних методів. Новизною роботи є те, що вперше пропонується використовувати в одній системі поєднання статистичних та експертних методів прийняття рішень, що дає змогу вирішувати нестандартні задачі в сфері інформаційної безпеки та робити порівняння результатів, отриманих різними методами, для вибору оптимального рішення.

Дослідження програмних СППР показало, що в залежності від методів обробки інформації їх умовно можна розділити на статистичні та експертні. Порівняльний аналіз таких програмних продуктів, як «Логос», «Net ModelKit Suite», «OLAP + CHART ModelKit», «Мыслитель» довів, що вони використовують або кількісні методи оцінки підтримки прийняття рішень, що в загальному базуються на статистичних даних з таблиць баз даних, або якісні методи оцінки підтримки прийняття рішень. Тобто для вирішення складних задач потрібно використовувати одночасно дві системи різного типу, що не завжди є зручно.

В даній роботі пропонується СППР яка складається з основних компонентів: бази даних, бази знань, модуля експерта бази даних, генератора даних та конструктора звітів. В базі знань знаходяться методи обробки інформації (основної статистики, кореляційного аналізу, багатовимірного шкалювання, класифікації, бальний та метод «позиційний радар»). Особа, що приймає рішення працює безпосередньо з модулем експерта баз даних та з конструктором звітів. Всі розрахунки проводяться в модулі «генератор даних». Можливість формування звітів дозволяє в зручному вигляді подати результати.

Дана система була реалізована програмно та протестована. Проведено порівняння розробленого програмного засобу з існуючими аналогами, яке показало його переваги за рахунок використання комбінованих між собою методів підтримки прийняття рішень. Дана система може бути використана для вирішення різного типу задач в сфері управління інформаційною безпекою.

Науковий керівник — к.т.н. Микола Тимошенко

Метод контролю функціонування механізмів захисту інформації

УДК 004.056.53 (043.2)
Ольга Клепач
Національний авіаційний університет, Україна, klepacholga@mail.ru

Проблема забезпечення безпеки автоматизованих систем (АС) одна з найбільш важливих та складних проблем в області автоматизованої обробки інформації. При використанні автоматизованої системи, існує потенційна загроза нанесення шкоди законним власникам і користувачам цих АС.

Постає задача забезпечення логічної безпеки компонент АС від несанкціонованого доступу, навмисних і ненавмисних помилок в діях людей та програм, які можуть спричинити збитки.

Необхідність контролю коректності програм зумовлена тим, що вони можуть служити каналом несанкціонованого доступу (НСД) до інформації.

Для забезпечення ефективності, контроль коректності повинен реалізовувати, як контроль функціонування самої системи захисту, так і контроль за діями користувача, що дозволить виробляти реакцію системи захисту та відсікати спроби несанкціонованих дій користувачів по відношенню до неї.

Розглянемо, як обидва напрямки реалізуються запропонованим методом контролю. Контроль над діями користувачів має на увазі деяку послідовність дій, кожну з яких можна характеризувати відповідним списком дозволених подій, або заборонених подій. Такими списками можуть бути: список зареєстрованих у системі користувачів; список заборонених до запуску процесів; список заборонених подій в системі; список пристроїв, до яких дозволений доступ користувачам. Контроль коректності функціонування системи захисту відбувається таким же чином, як і контроль над діями користувачів. При цьому регламентуються дії не користувачів, а самої системи захисту. Складаються списки санкціонованих подій-еталонів, з якими періодично порівнюються поточні події. Система захисту вважається порушеною у разі розбіжності еталонної копії і оригіналу.

У відповідь ініціюється відповідна реакція системи: завершення несанкціонованого процесу; завершення сеансу несанкціонованого користувача в системі.

Відмінною особливістю розглянутого підходу є те, що не важливо, яким чином зловмисник намагається здійснити НСД до інформації, тому що фіксуються не конкретні описи, а непрямі ознаки атаки – несанкціоновані для системи події.

Запропонований метод контролю коректності механізмів захисту інформації може бути використаний при програмній розробці з метою введення додаткового рівня захисту.

Науковий керівник — д.т.н. Володимир Хорошко

Програмний комплекс тестування комп'ютерних систем на проникнення

УДК 004.056(043.2)
Юлія Коваленко, Єгор Соколов
Національний авіаційний університет, Україна, ivanchyk_81@mail.ru, yegorsokolov@mail.ru

В результаті активного розвитку інформаційних технологій за останні роки рівень кібернетичних атак значно виріс. На даний момент існує багато методів захисту інформації від несанкціонованого доступу. На нашу думку найефективнішим методом захисту є «тестування на проникнення».

Тестування на проникнення (penetration testing, pentest - тести на подолання захисту) виступає як детальний аналіз мережі і систем з точки зору потенційного зловмисника. Суть тесту полягає в санкціонованій спробі обійти існуючий комплекс засобів захисту інформаційної системи. Тест на проникнення дозволяє отримати об'єктивну оцінку того, наскільки легко отримати доступ до ресурсів корпоративної мережі або сайту компанії, яким способом і через які вразливості.

Сучасні розробки у галузі захисту інформації розглядають основне завдання будь-якої КСЗІ як протидія розподіленим атакам. Атакою на комп'ютерну систему називається дія або послідовність зв'язаних між собою дій порушника, які приводять до реалізації загрози шляхом використання вразливостей цієї комп'ютерної системи. Очевидно, що для підвищення ефективності КСЗІ необхідно мати формальне опис можливих дій порушників, а також способів їх реалізації.

Для успішної реалізації атаки зловмисник повинен виконати розвідку об'єкта нападу з метою пошуку вразливостей, які можуть бути використані в майбутньому.

Метою дослідження є виявлення слабких місць в захисті інформаційної системи. Згідно мети дослідження було розглянуте завдання: розробити модель процесу формування інформаційних загроз в АС.

Тестування на проникнення дозволяє отримати об'єктивну оцінку того , наскільки легко здійснити несанкціонований доступ до ресурсів корпоративної мережі або сайту вашої компанії , яким способом , через які уразливості або через які недоробки в системі.

Проведення тестів на проникнення дозволяє перевірити рівень захищеності систем і рівень зрілості СУІБ .

Зовнішній тест на проникнення виконується із загальнодоступних мереж і моделює поведінку зловмисника , нападника з Інтернет (як з використанням соціальної інженерії , так і без неї). Зовнішні тести на проникнення розрізняються за обсягом спочатку наданої інформації фахівцеві , що виконує тест.

В результаті проведеного тесту на проникнення ми можемо отримати реальний погляд на рівень інформаційної безпеки компанії. А також скласти рекомендації щодо підвищення рівня захищеності інформаційної системи.

Модель системи менеджменту інцидентів інформаційної безпеки

УДК 004.056:004.891
Іванна Кірик, Віктор Гнатюк
Національний авіаційний університет, Україна, Kiryk_ivanna@mail.ru, viktorgnatyuk@ukr.net

Сьогодні кіберзлочинність набуває глобального характеру і потребує об'єднаних дій для боротьби з нею. Для захисту від кібератак кожна компанія намагається застосовувати найбільш ефективні та продуктивні системи і моделі захисту інформації. Необхідно зауважити, що основним завданням систем менеджменту, які забезпечують цілісність даних в організації є своєчасне та оперативне реагування на кібератаки в інформаційно-комунікаційних системах (ІКС), виявлення та уникнення появи інцидентів, визначення шляхів усунення їх наслідків і розробка превентивних заходів. Проте універсальної системи, яка б задовольняла всі вимоги керівників і забезпечувала безперебійну роботу, немає.

Тому надзвичайно актуальним є розробка програмного засобу NAU Service Desk, який буде адаптований відповідно до вимог вищого навчального закладу та загроз безпеці його ІКС.

Метою роботи є підвищення рівня захищеності ІКС організації, за рахунок розробки системи NAU Service Desk, що надасть можливість покращити якість обслуговування користувачів шляхом автоматизації роботи служби технічної підтримки.

Сучасний ринок програмних комплексів, щодо виявлення інцидентів досить насичений. Всі програмні продукти різняться своїм функціоналом та можливостями. Але більшість систем мають основні недоліки, такі як різні програмні платформи, відсутність шаблонів. Найпоширенішим недоліком є висока вартість програмного продукту.

Аналіз ринку програмного забезпечення показав, що найкращим рішенням для університету буде шлях розробки системи реєстрації та обробки заявок своїми силами. Система NAU Service Desk – це гнучкий додаток, який здатен не тільки адаптуватися до вирішення поточних потреб в умовах обмеженості ресурсів, а й з'єднуватися з вже існуючими службами багатокомпонентної інформаційної системи.

За допомогою даного продукту, будуть мінімізовані часові та матеріально технічні ресурси, що витрачаються на усунення проблем; всі заявки, які поступили в систему, будуть зібрані в єдиному електронному журналі заявок; сформований електронний архів виконаних заявок; налагоджено автоматичну реєстрацію заявок, які надійшли в неробочий час при відправленні їх через веб-форму; використання шаблонів та ін..

В результаті, була розроблена NAU Service Desk, яка була створена відповідно до вимог вищого навчального закладу, і містить в собі всі необхідні інструменти та функції, які необхідні для нормалізації та полегшення роботи працівників університету.

Науковий керівник — к.т.н. Сергій Гнатюк

Програмна система захищеного інтерактивного обміну даними

УДК 004.056
Андрій Шевчук
Національний авіаційний університет, Україна, shevchuk@be-aware.com.ua

На сьогоднішній день дуже велику роль у сфері діяльності компаній відіграє цілісність та захищеність їхніх даних. На сам перед, це ті дані, які стосуються користувачів ресурсу (паспортні дані, платіжна інформація, місце проживання, тощо), та конфіденційне листування між клієнтами та співробітниками, саме тут и постає питання в безпечному та швидкому обміні даними. Краще за все для цього підходить глобальна мережа інтернет. Але інтернет сам по собі ніколи не був безпечним, а навпаки, будь-які дані, які колись потрапляють до цієї мережі, більше з неї не зникають і можуть бути викрадені, та використовуватись для фальсифікації клієнтів, що в свою чергу дуже згубно впливає на репутацію ресурсу. Саме в цьому є вирішення актуального питання - безпечне транспортування та зберігання даних між клієнтом та кінцевим ресурсом через веб-сайт.

Метою роботи є побудова програмного модуля інтерактивного обміну даними. Для досягнення цієї мети необхідно визначити наступні задачі. Проаналізувати існуючі програмні застосунки, методи та засоби захисту використовувані в них для безпечного обміну даними. На основі цих даних розробити програмний модуль та промоделювати його роботу для захисту обміну даними.

Новизною є застосування вдосконаленого методу для безпечного обміну даними за рахунок поєднання криптоалгоритмів, що дасть можливість підвищити надійність та зберегти цілісність інформації, що підлягає інтерактивному обміну.

В ході роботи було проаналізовано декілька програм для безпечного обмінну даними, та виявлені деякі недоліки. До списку програм увійшли такі відомі месенджери, як “Skype” та “Viber”. В результаті було вирішено використовувати “WebSocket” з “SSL” для роботи браузеру з веб-ресурсом. Це забезпечує первинний захист даних обміну між клієнтом і ресурсом. Після вдалої ініціалізації з’єднання клієнті по черзі генерують на своїй стороні ключі для шифрування повідомлень і передають публічну частину, для шифрування повідомлень які адресовані йому. Також до кожного повідомлення додається хеш, за допомогою якого можна дізнатися чи не було повідомлення модифіковане. Завдяки цій схемі, збільшується надійність захищеності даних орієнтовно на 10 відсотків.

Результатом даної роботи є безкоштовний модуль захищеного інтерактивного обміну даними, який можна з легкістю встановити на будь який ресурс.

Науковий керівник — к.т.н. Євгенія Іванченко

Система захисту інформації на основі операцій розширеного матрично-криптографічного перетворення

УДК 004.056.55.(043.2)
Артем Баранов
Національний авіаційний університет, Україна, Art5131992@maul.ru

Колективне використання інформаційних ресурсів потребує відповідного захисту дисків і каталогів, окремих папок і файлів, а також усіх локальних і глобальних мереж від несанкціонованого втручання інформаційних зловмисників, вірусів і небезпечних програм. Тому важливою проблемою є постійне підвищення стійкості систем захисту інформації. Одним із основних напрямків розвитку систем захисту інформації є криптографічний захист.

Проте в сфері захисту інформації залишається цілий ряд задач і проблем, вирішення яких має важливе науково-технічне й загальнодержавне значення. Однією з таких задач є підвищення стійкості систем захисту інформації на основі використання операцій розширеного матричного криптографічного перетворення (РМКП) для інформаційних систем.

Метою роботи є підвищення стійкості систем захисту інформації на основі використання операцій РМКП для захисту конфіденційної інформації.

Для досягнення поставленої мети було проведено аналіз існуючих криптографічних методів та засобів захисту інформації, за результатами якого визначено нову групу операцій криптографічного перетворення, яка забезпечить підвищення криптостійкості систем захисту інформації. Для забезпечення збору інформації про логічні функції декількох змінних, які можуть використовуватися в криптографії, та визначення їх особливостей використовувалась методика синтезу логічних функцій на основі методу перебору.

Запропонована концепція РМКП, яка теоретично базується на експериментально доведеному факті, що операції матричного криптографічного перетворення (МКП) та РМКП не утворюють групи операцій криптографічного перетворення. Як наслідок, повторне трансформування інформації операціями з іншої групи криптографічних операцій забезпечує підвищення криптографічної стійкості. Виходячи з запропонованої концепції для забезпечення високої криптографічної стійкості, операції РМКП використовуються сумісно з операціями МКП, і забезпечують попередню або подальшу обробку даних.

При розробці системи захисту інформаційних ресурсів на основі розширених матричних операцій криптографічного перетворення взято метод захисту інформаційних ресурсів на основі матричних операцій криптографічного перетворення. Розширене РМКП залежно від параметрів nk і Коп дає змогу збільшити криптостійкість від 1032 до 10150 разів пропорційно відносно потокового шифрування при зменшенні часу шифрування від 1,5 до 6 разів. Реалізація операцій РМКП відповідає вимогам програмного пакета статистичного тестування NIST STS.

Науковий керівник — к.т.н. Анна Корченко

Метод біометричної аутентифікації в інформаційно-комунікаційних системах

УДК 57.087.1:683.336.2:351.814.2(043.2)
Анастасія Бородуліна
Національний авіаційний університет, Україна, sapfirra08@mail.ru

Проблеми інформаційної безпеки (ІБ) інформаційно-комунікаційних систем (ІКС) на суб'єктах цивільної авіації (ЦА) в нинішніх умовах є невід'ємною частиною діяльності усієї авіаційно-транспортної системи держави. Більше того, у низці випадків вони стали найважливішими завданнями забезпечення гарантованого рівня безпеки польотів. Активне обговорення питань забезпечення інформаційної безпеки ІКС у ЦА, що проходить на конференціях та нарадах ІКАО, свідчать про велику актуальність багатьох ключових проблем, пов'язаних з серйозними руйнівними наслідками при порушенні ІБ, недостатньою ефективністю засобів захисту тощо.

Керівні документи з авіаційної безпеки містять опис заходів, які необхідно здійснювати для захисту критичних авіаційних систем (КАІС) від кіберзагроз, зокрема зазначено, що до таких систем (тобто КАІС) відносяться і системи контролю доступу. Крім того, акцентується увага на доцільності застосування багаторівневого підходу, який, крім іншого, включає в себе впровадження систем аутентифікації, зокрема на основі використання біометричних методів, з метою забезпечення доступу до КАІС виключно легітимним користувачам. Але не всі біометричні методи захисту підходять для застосування у таких системах (зважаючи на їх критичність). З огляду на це, актуальним науковим завданням є розробка та дослідження біометричних методів аутентифікації, що задовольнятимуть вимоги безпеки КАІС. Таким чином, метою роботи є забезпечення захисту критичних авіаційних інформаційних систем шляхом удосконалення методу біометричної аутентифікації користувачів.

Для досягнення поставленої мети необхідно було вирішити такі завдання: провести аналіз існуючих методів біометричної аутентифікації, визначити їх переваги, недоліки та відповідність вимогам безпеки КАІС; удосконалити метод біометричної аутентифікації користувачів (за рахунок оптимізації алгоритму виділення зовнішніх границь ока та зіниці); реалізувати програмно та експериментально дослідити роботу удосконаленого методу щодо його здатності забезпечувати аутентифікацію в КАІС.

Дослідивши низку наукових джерел, встановлено, що існує досить велика кількість методів біометричної аутентифікації. Основними методами, що використовують статистичні біометричні характеристики людини, є ідентифікація за папілярним малюнком на пальцях, райдужною оболонкою, геометрією особи, сітківкою ока, малюнком вен руки тощо. Також існує низка методів, що використовують динамічні характеристики людини: ідентифікація за голосом, динамікою рукописного почерку, серцевим ритмом, ходою та ін. Аналіз показав, що методи аутентифікації за динамічними характеристиками є досить ненадійними, особливо в випадках, коли мова йде про такі критичні системи, як КАІС. Методи, що базуються на статичних характеристиках, є значно надійнішими. Для їх оцінки використовуються дві основні характеристики (параметри) будь-якої біометричної системи – FAR

(ймовірність помилкового збігу біометричних характеристик двох людей) і FRR (ймовірність відмови доступу людині, що має допуск). У табл. 1 наведено значення цих параметрів для різних біометричних методів. Крім того, оцінка може проводитися за додатковими параметрами, такими як стійкість до підробки, стійкість до навколишнього середовища, простота використання, вартість, швидкість, стабільність ознаки в часі тощо.

Таблиця 1 — Аналіз методів біометричної аутентифікації.

Метод	FAR	FRR
Відбитки пальців	0,001 %	0,6%
Райдужна оболонка ока	0,00001 %.	0,13% – 0,19%
Сітківка ока	0,001%	0,4%
Геометрія обличчя 2D	0,1 %	2,5%
Геометрія обличчя 3D	0,0047%	0,103%
Геометрія рук	0,1%	0,1%
Венозний малюнок руки	0,0008 %	0,01 %

Як видно із табл. 1, найефективнішим серед зазначених методів є аутентифікація за райдужною оболонкою ока. На практиці такий метод реалізується кількома алгоритмами, найкращим серед яких є алгоритм Даугмана. Цей алгоритм спочатку уточнює центр зіниці і межі райдужної оболонки, розглядаючи частину кругового контуру, потім використовує вейвлет перетворення Габора щоб витягти фазову структуру райдужної оболонки (рис. 1). Остання кодується в дуже компактному бітовому потоці та зберігається у базі даних для ідентифікації.

Алгоритм Даугмана, на відміну від багатьох інших, є безпараметричним і показує високу ефективність (93,5% коректних розпізнавань), однак і він має низку проблем, які були враховані при вдосконаленні методу.

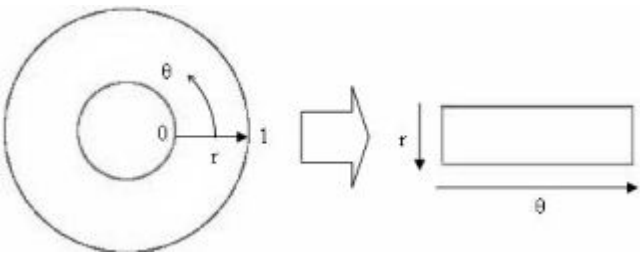

Рис. 1. Нормалізація зображення райдужної оболонки ока

Таким чином, удосконалений метод біометричної аутентифікації (за зображенням райдужної оболонки ока), за рахунок оптимізації алгоритму виділення зовнішніх границь ока та зіниці, дозволяє підвищити точність ідентифікації користувачів й оптимізувати основні характеристики системи біометричної аутентифікації (FAR і FRR). З огляду на це, він може використовуватись у КАІС для підвищення ефективності роботи систем аутентифікації та контролю доступу.

Науковий керівник — к.т.н. Сергій Гнатюк

Криптографічний модуль захисту інформації на основі удосконаленого алгоритму шифрування CLEFIA

УДК 003.26:004.056.55
Юлія Гаврилюк, Василь Кінзерявий
Національний авіаційний університет, Україна, qyuliaq@mail.ru, 0werl0rd@ukr.net

У наш час значно збільшилася сфера використання комп'ютерних мереж. Сьогодні за допомогою комп'ютерних мереж із використанням криптографічних методів передаються великі обсяги інформації різного характеру (військового, державного, особистого і комерційного), що не дає змоги стороннім особам отримати доступу до неї. Проте, виникнення сучасних надпотужних комп'ютерів, поява технологій нейронних і мережевих розрахунків робить можливим дискредитацію систем шифрування, які ще нещодавно вважалися цілком безпечними. Саме тому завдання вдосконалення методів шифрування в обчислювальних системах є особливо актуальним.

Метою даної роботи є підвищення ефективності криптографічного захисту інформаційних ресурсів шляхом розробки криптографічного модуля на основі удосконаленого алгоритму шифрування CLEFIA.

На сьогодні існують блокові симетричні шифри (БСШ), які забезпечують високий (гарантований) рівень стійкості і які знайшли широке розповсюдження (наприклад: алгоритм AES, Camellia, SEED). В процесі їх впровадження на практиці виявилось, що для деяких додатків вони є складними в реалізації і не забезпечують необхідних показників швидкодії. Зважаючи на це, були розроблені нові БСШ, які отримали назву полегшених. Зміст полегшеності в тому, що в них зменшена складність криптографічних перетворень. Одним з таких БСШ є CLEFIA. CLEFIA являє собою розширену схему Фейстеля, в якій 128-бітний інформаційний блок розбивається на 4 підблоки над якими виконуються раундові перетворення. У алгоритмі CLEFIA може використовуватись секретний ключ розміром 128, 192 або 256 біт та виконуються відповідно 18, 22, або 26 раундових перетворення.

У роботі побудований швидкісний криптографічний модуль, заснований на удосконаленому алгоритмі шифрування CLEFIA. Оригінальна структура алгоритму була збережена, проте було введено ряд змін: 1) збільшено довжину вхідного блоку даних до 256 біт; 2) виконується повне початкове і кінцеве забілювання блоку даних; 3) у функції F використовуються динамічно змінювані таблиці замін; 4) змінено операцію лінійного розсіювання; 5) спрощено процедуру розширення секретного ключа; 6) зменшено кількість раундів.

Проведено дослідження, яке показало, що удосконалений алгоритм шифрування CLEFIA пройшов комплексний контроль за методикою NIST STS. Також показано, що швидкісні характеристики криптографічного модуля на основі удосконаленого алгоритму CLEFIA покращились на 10% порівняно із аналогічним модулем на основі оригіналу. Проте, існує необхідність подальшого дослідження стійкості удосконаленого алгоритму CLEFIA до відомих видів атак.

Програмний модуль захисту електронних інформаційних ресурсів в системі реального часу QNX

УДК 0004.421.5:03.26:004.056.55
Рустам Хазраті, Василій Кінзерявий
Національний авіаційний університет, Україна, khazrati@bigmir.net

Однієї з найважливіших областей застосування обчислювальної техніки є обмін інформацією. Управління енергопостачальними об'єктами, управління автоматизованими системами – це та багато іншого входить до списку задач систем реального часу. Через високу складність та значимість виконуваних задач виникає потреба в особливих вимогах до програмного забезпечення: надійність, висока пропускна здатність, своєчасна реакція на зовнішні чинники. Разом з тим захист електронних інформаційних ресурсів в системах реального часу потребує виключної уваги. Одним із можливих способів захисту електронних інформаційних ресурсів є криптографічний захист. Не дивлячись на різноманіття існуючих криптографічних алгоритмів, дослідження, спрямовані на розробку нових та удосконалення вже існуючих алгоритмів, ніколи не втратять своєї актуальності.

Основною метою роботи є підвищення ефективності криптографічного захисту електронних інформаційних ресурсів в системі реального часу QNX за допомогою розробки програмного модуля на основі удосконаленого алгоритму шифрування Blowfish.

Алгоритм шифрування Blowfish був розроблений Брюсом Шнайером ще у 1994 році. Серед його переваг можна виділити наступне: висока швидкість шифрування (якщо не потрібно часто змінювати секретний ключ), простота алгоритму, відсутність відомих успішних атак на повнораундову версію алгоритму, що виконуються за розумний час. До недоліків відносять: процедура розширення секретного ключа є ресурсоємкою, невеликий розмір блоку даних, теоретична вразливість до диференціального криптоаналізу.

Запропонований програмний модуль побудовано на базі удосконаленого криптографічного алгоритму Blowfish. Удосконалений Blowfish отримав декілька нововведень порівняно із оригіналом: 1. Збільшилась довжина блока даних – із 64 біт до 256 біт. 2. Використовується нова послідовність операцій у функції F мережі Фейстеля. 3. Зменшилась кількість раундів – з 16 до 12. 4. Змінено процедуру розширення секретного ключа. 5. Використовуються фіксовані блоки підстановок (використовуються 4 таблиці замін, які вибрані з гранично-нелінійних бієктивних перетворень).

Експериментальне дослідження показало, що розроблений програмний модуль на базі удосконаленого алгоритму шифрування Blowfish дав змогу підвищити швидкість на 25% в порівнянні з його оригінальним варіантом. Також, у середовищі статистичних тестів NIST було доведено, що послідовності утворені запропонованим модулем є псевдовипадковими. Далі планується дослідити стійкість удосконаленого Blowfish до різних методів криптоаналізу.

Науковий керівник – к.т.н. Анна Корченко

Програмний засіб для гарантованого видалення даних з інформаційних носіїв

УДК 004.421.5: 004.056.55 (043.2)
Каріна Безверха, Василь Кінзерявий
Національний авіаційний університет, Україна, karina0kira@ukr.net, 0werL0rd@ukr.net

У даний час більшість організацій прийшли до розуміння значення захисту інформації і впроваджують засоби, що дозволяють забезпечити безпеку інформації на різних етапах її життєвого циклу. Однак останньому етапу − утилізації інформації часто приділяється недостатньо уваги. Можна виділити два основні канали витоку залишкової інформації, що виникають внаслідок її недостатньо надійного видалення. Першим з них є витік інформації при заміні інформаційних носіїв. Другим є несправні накопичувачі. За статистикою компанії Ontrack, що займається відновленням інформації з жорстких дисків (ЖД) − в 56% випадків втрати даних винні апаратні збої жорстких дисків.

Актуальність роботи викликана тим, що при не вчасному чи не надійному знищенні даних з ЖД, конфіденційна інформація стане доступною стороннім особам навіть після її знищення, що може привести до негативних наслідків.

Метою дипломної роботи є підвищення ефективності гарантованого видалення даних з інформаційних носіїв шляхом використання запропонованого методу зберігання та видалення даних із інформаційних носіїв.

Проведений аналіз показав, що сьогодні існує чимало програмних засобів (ПЗ) для гарантованого видалення інформації, відмінність між якими заключається в наборі методів видалення та специфіці затирань даних. Більшість методів спеціалізується на великій кількості циклів затирань і тому видалення великого об'єму даних займає багато часу. У зв'язку з цим, було вирішено розробити швидкісний (ПЗ), що гарантовано видаляв дані з носіїв інформації. Для цього було проаналізовано сучасні міжнародні стандарти (US DoD 5220.22-M, США NAVSO P-5239-26, VSItR, ГОСТ R 50739-95) у галузі забезпечення інформаційної безпеки щодо гарантованого знищення даних. На основі проведеного аналізу запропоновано метод зберігання та видалення даних із інформаційних носіїв, суть якого полягає у наступному: 1. Усі файли на інформаційному носії зберігаються у зашифрованому вигляді. При виконанні будь-якої операції з файлом – він спочатку розшифровується, а при зберіганні змін виконується його шифрування розробленим швидкісним алгоритмом шифрування. 2. Секретні ключі для кожного файлу зберігаються у захищеному файлі. При кожному зберіганні файлу для нього генерується новий секретний ключ. 3. Для гарантованого видалення файлу достатньо видалити його секретний ключ із захищеного файлу. На основі запропоновано методу зберігання та видалення даних із інформаційних носіїв було розроблене відповідне ПЗ. при використанні якого забезпечується гарантоване видалення даних з інформаційних носів та стійкість відносно (ПЗ), що спеціалізуються на відновленні знищених даних.

Науковий керівник – к.т.н. Олексій Гавриленко

Криптографічний модуль передачі даних на основі удосконаленого поточного шифру Trivium

УДК 003.26:004.056.55
Василь Кінзерявий, Аліна Синюта
Національний авіаційний університет, Україна, ccaatt2008@ukr.net

З розвитком інформаційних технологій все більшого розмаху набуває проблема захисту інформаційних ресурсів, які передаються та зберігаються в інформаційно-комунікаційних системах. Криптографічний захист на протязі всього часу розвитку цивілізації був одним з найбільш перспективних і актуальних методів забезпечення інформаційної безпеки. Ефективність криптографічного захисту в першу чергу оцінюється стійкістю і швидкістю використовуваних методів. Із стрімким розвитком інформаційних технологій вимоги до цих параметрів значно зростають. Тому, актуальним завданням є розробка нових та удосконалення існуючих криптографічних методів з метою підвищення ефективності захисту електронних інформаційних ресурсів.

Основною метою даної роботи є підвищення ефективності криптографічного захисту інформаційних ресурсів шляхом розробки криптографічного модуля передачі даних на основі удосконаленого поточного шифру Trivium.

Trivium − симетричний алгоритм синхронного потокового шифрування, орієнтований, в першу чергу, на апаратну реалізацію з гнучким рівновагою між швидкістю роботи і кількістю елементів та має можливість достатньо ефективною програмної реалізації. Шифр був представлений в грудні 2008 року як частина портфоліо європейського проекту eSTREAM. Даний потоковий шифр генерує до 264 біт вихідного потоку з 80 біт ключа і 80 біт вектора ініціалізації. Trivium включений в стандарт ISO / IEC 29192-3 в якості легковагого потокового шифру.

У роботі розроблено програмний модуль передачі даних на основі удосконаленого потокового шифру Trivium. Суть його удосконалення полягає у наступному: 1. Використовуються не 3, а 4 регістри зсуву. Додатково був введений 128 бітний регістр. 2. Усі операціх виконуються над 32 бітними словами. 3. При вироблені нових елементів гами використовується динамічно змінювані таблиці підстановок. 4. Збільшено ромір ключа та ветора ініціалізації до 256 біт.

Властивості послідовностей утворених удосконаленим шифром Trivium досліджувалися у середовищі тестів NIST STS. Згідно з результатами дослідження, удосконалений шифр Trivium проходить всі 188 тестів та показує не гірші результати за еталонний генератор BBS.

Крім того було проведено експериментальне дослідження швидкісних харатеристик програмних модулів на основі оригінального шифру Trivium та його удосконаленої версії (за однакових умов), які показали, що швидкість удосконаленого поточного шифру Trivium краще на 17% ніж в його оригінальному варіанті. Далі планується провести дослідження щодо обгрунтування його стійкості до відомих методів криптоаналізу.

Науковий керівник - к.т.н. Сергій Гнатюк

Комплексна система захисту інформації інтернет-провайдера

УДК 004.056(043.2)
Юрій Стародуб, Василь Кінзерявий
Національний авіаційний університет, Україна, yurii.starodub.ua@ieee.org, 0werL0rd@ukr.net

Необхідність забезпечення захисту інформації шляхом створення комплексної системи захисту інформації визначається законодавством України, а в деяких випадках власником інформаційних ресурсів. Це особливо актуально для підприємств де зберігаються персональні дані десятків, а іноді і сотень тисяч користувачів. До того ж розвитком інформаційних систем все більша кількість пристроїв підключається до глобальної мережі інтернет - це не лише персональні комп'ютери, лептопи та сервери, а й принтери, телефони, планшети та інше обладнання. Також в багатьох організаціях та компаніях широко розповсюджуються тренди Bring Your Own Device (BYOD), online collaboration та хмарні обчислення, що вимагає впровадження нових політик доступу, які будуть передбачати згоду користувачів виконувати правила використання власних пристроїв для доступу до корпоративних ресурсів та з відповідальністю за їх порушення та інші аспекти .

Для інтернет-провайдера є актуальним питання забезпечення доступності сервісів для своїх клієнтів, конфіденційність їх персональних даних та цілісності інформації, що передається в мережі. Враховуючи що засоби реалізації атак не стоять на місці, вони еволюціонують, комбінуються та об'єднуються в комплекси для підвищення ефективності неправомірних дій метою яких є порушення конфіденційності, цілісності та/або доступності ресурсів, варто використовувати комплексний підхід для забезпечення захищеності системи. Для зменшення ризику інформаційної безпеки було вирішено розробити комплексну систему захисту інформації (КСЗІ) приватного підприємства для автоматизованої системи (АС) 3 класу. Впровадження КСЗІ дозволить забезпечити безпеку критичної інформації та інформаційних ресурсів у процесі функціонування АС, мінімізувати, а в деяких випадках уникнути втрат від можливих загроз. Для цього було проведено оцінку ризиків та інформаційних ресурсів підприємства, розроблено технічне задання КСЗІ.

В ході роботи було проаналізовано понад десять нормативно-правових документів, серед них Закони України у сфері телекомунікацій та захисту інформації, НД ТЗІ та інші Також було проаналізовано 2014 Internet Security Threat Report - звіт представлений Symantec Global Intelligence Network та Global Corporate IT Security Risks: 2013 опублікований Kaspersky Lab.

Результати даної роботи дозволять забезпечити захищеність інформаційних ресурсів підприємства, а набутий досвід може бути використаний для підтримки захищеності системи та для побудови нових КСЗІ.

Науковий керівник - к.т.н. Євгенія Іванченко

Програмний застосунок підтримки процесу побудови моделі загроз

УДК 004.056(043.2)
Юрій Заремба
Національний авіаційний університет, Україна, yurii.zaremba@gmail.com

Розглядаючи інформацію як об'єкт діяльності, треба відзначити, що залежно від її важливості та значення для користування нею витрачають відповідні ресурси. Але важливість та значення інформації для тих чи інших суб'єктів інформаційних відносин в умовах прихованого комерційного, відомчого та державного інтересу визначити складно. Тому зрозуміло, що задоволення інформаційних потреб перебуває в пропорційній залежності від умов та методів (засобів) практичної діяльності відповідних суб'єктів, а високий рівень автоматизації, до якого прагне людство, ставить його в залежність від рівня безпеки інформаційних технологій, які воно використовує. Загроза інформаційної безпеки інформаційного простору – це можливість реалізації впливу на інформацію, що призводить до створення, знищення, копіювання, блокування доступу до інформації, а також впливу на компоненти інфраструктури інформаційного простору, що призводить до втрати знищення або збою функціонування носія інформації, засобів взаємодії з носієм або засобів управління ним. Необхідність класифікації загроз інформаційної безпеки (ІБ) обумовлена тим, що архітектура сучасних засобів автоматизованої обробки, організаційна, структурна та функціональна побудова інформаційно-обчислювальних систем (мереж), технології та умови обробки такі, що інформація підлягає впливу надмірно великої кількості факторів, за якими і потрібно формалізувати задачу опису загроз та ефективної протидії їм. Виходячи з технології обробки інформації та побудови моделі загроз (МЗ) інформації, для того, щоб прискорити та структурувати процес розробки комплексної системи захисту інформації (КСЗІ), необхідно розробити програмний модуль підтримки процесу побудови МЗ, який на основі вказаних експертом з ІБ параметрів, у вигляді автоматизованого звіту, відображатиме основні характеристики загроз та розподілятиме наявні загрози за класами. У зв'язку з цим метою роботи є визначення основних складових компонентів МЗ та створення програмного застосунка підтримки процесу побудови МЗ, який дозволить спростити процес розробки такої моделі. Визначення складових компонентів МЗ здійснюється на основі аналізу документації з оцінки захищеності інформації та побудови КСЗІ. Представлений програмний застосунок побудови МЗ дозволяє в автоматизованому режимі будувати МЗ для будь-якої організації. Будова системи досить проста, вона складається із бази даних інформаційних ресурсів організації, бази даних загроз, модуля аналізу та оцінювання ризиків та модуля генерації звіту «Модель загроз». Розробка програмної системи підтримки побудови МЗ проводилася з метою оптимізації роботи експертів із оцінки захищеності інформаційних ресурсів в КСЗІ. Результатом роботи цієї системи є електронний звіт, який повністю відображатиме історію відповідей експерта на питання стосовно захищеності КСЗІ, клас та детальний опис характеристик визначених загроз. *Науковий керівник — к.т.н. Микола Тимошенко*

Модуль захисту web-сайту від несанкціонованого доступу

УДК 004.056
Андрій Бородій
Національний авіаційний університет, Україна, aborodiy@space-it.com.ua

Більшість сайтів використовують відомі та поширені засоби захисту інформації. Тому зловмисникам простіше отримати потрібні дані, адже методи захисту та їх алгоритми вже вивчені. Це дає можливість використовувати вразливі місця таких алгоритмів з метою проведення атаки на сайт. З огляду на це, розробка програмного модуля захисту Web-сайту від несанкціонованого доступу є актуальним завданням.

Метою роботи є розробка програмного модулю захисту Web-сайту від несанкціонованого доступу. Новизною є удосконалення методу графічної авторизації, за рахунок використання алгоритму, що базується на графічній авторизації.

Під час виконання роботи було розроблено програмний модуль захисту веб-сайту від несанкціонованого доступу на основі покращеного алгоритму з використанням графічної авторизації. Вдосконалення відбулося за рахунок використання алгоритму графічної авторизації та впровадження його в сфері web-програмування. Інтегрувавши даний алгоритм в загальну систему захисту, вдалося значно розширити ключовий простір, а також час, який необхідний для зламування пароля методом «простого перебору». Реалізація даного методу є надзвичайно простою, оскільки основана на базових поняттях мови HTML, проте і водночас дуже надійною. Якщо провести нескладні обчислення, то можна з впевненістю сказати, що розмір зображення відіграє ключову роль стійкості даного алгоритму до перебору пароля: чим більша площа зображення, тим більший ключовий простір. Можна описати залежність ключового простору від площі зображення: $K = S/100$, де K – це кількість варіантів, а S – це площа зображення. Це також являється своєрідним недоліком даної системи.

Також розроблений модуль має стійкість до атак типу «людина посередині», адже для передачі даних між користувачем та сервером використовується криптоалгоритм AES-128, який являється швидкодіючим та надійним, що є головними критеріями його використання для Web-застосунків. Розподіл ключів для шифрування забезпечується на основі використання тимчасового, або сесійного ключа, який формується випадковим чином для кожного користувача і є стійким до підбору.

Програмний модуль було досліджено утилітою CyD Network Utilities, за такими критеріями, як вразливість до атак типу XSS, SQL-injection, includes, а результати тестування є задовільними.

Розроблений алгоритм є лише альтернативним способом системи авторизації на сайті, проте при подальшому його вдосконаленні можливо досягти надзвичайної стійкості до атак.

Науковий керівник — к.т.н. Микола Тимошенко

Програмний модуль захисту web-сайту інтернет-магазину

УДК 004.056

Єльмар Мірзоев
Національний авіаційний університет, Україна, elmarplanet@rambler.ru

Кількість зломів Web-сайтів в Україні істотно зросла за останні кілька років. Слабке місце більшості українських Web-сайтів у тому, що вони не знають хакерських можливостей країни. Більшість підприємств не знають, що чекає їх та їхній Web-ресурс у глобальній мережі. Здійснення атаки на Web-сайт може призвести до порушення режиму комерційної таємниці в компанії, до втрати іміджу та репутації, довіри як клієнтів, так і партнерів, і до прямих фінансових втрат. Тому розробка модуля захисту Web-сайту для інтернет-магазину є досить актуальним завданням.

Метою роботи є забезпечення захищеності Web-сайту інтернет-магазину шляхом розробки програмного модуля захисту. Новизною є розробка програми для забезпечення доступності Web-сайту із використанням сучасних методів захисту, що дасть можливість блокувати процес обходу аутентифікації.

У процесі виконання роботи був проведений аналіз та дослідження найпоширеніших загроз та вразливостей Web-сайтів. Виділено 6 класів, кожен з яких включає відповідні йому атаки. Було досліджено існуючі системи зихисту Web-сайтів. Кожен Web-додаток – додаткові вразливості. Тому краще впроваджувати власний модуль захисту, який засновано на всіх особливостях Web-сайту і можливих загрозах. І в такому випадку безпека розробленого Web-порталу буде залежати тільки від вас і вашої команди. Враховуючи специфіку комерційних підприємств, статистичні дослідження та факт адекватності безпеки, були побудовані структури трьох рівнів модуля захисту Web-сайту. Ці рівні відрізняються між собою ретельністю перевірки масивів даних, кількістю надання персональних даних користувачем, лояльністю модуля безпеки до дій користувача. Таким чином вони яскраво ілюструють варіації реалізації методів захисту від ідентичних загроз.

Було розроблено алгоритм та програмний модуль захисту Web-сайту, який включає у себе підсистему захисту від обходу аутентифікації (складові: модулі реєстрації та активації), що взаємодіє із підсистемою захисту від різного роду ін'єкцій, підсистемою захисту від піггібекінгу, підсистемою захисту від обходу авторизації, підсистемою захисту від прямого доступу до файлів, підсистемою захисту від неправомірного отримання куків і підсистемою захисту від XSS-атаки. Досліджено роботу розробленого модуля захисту Web-сайту. Реалізація модулів інтернет-магазину довела, що розроблена бібліотека функцій дозволяє уникнути громіздкості та надлишковості коду, легко змінити існуючий профіль та дописати свій власний. Зроблені перевірки показали, що зменшена можливість реєстрації програми-бота (у III рівні зведена до нуля), підбору пароля, реалізації піггібекінгу, обходу авторизації, XSS-атаки, несанкціонованого доступу до куків, унеможливлено реалізації різного роду ін'єкцій.

Науковий керівник — к.т.н. Євгенія Іванченко

Система менеджменту інформаційної безпеки міжнародного аеропорту

УДК 004.056

Ольга Сацюк
Національний авіаційний університет, Україна, olga.satsyuk@gmail.com

Загроза застосування актів кібертероризму в авіації зростає значно більш високими темпами, ніж засоби їх попередження. На даний момент питання кіберпезпеки є дещо другорядними у ЦА, проте проникнення нових технологій виводить інформаційну безпеку у найбільш вразливі категорії із забезпечення безпеки ЦА. Тим не менш, єдиних стандартизованих рекомендацій у протистоянні кіберзагрозам у ЦА на сьогоднішній день немає. Саме тому розробка системи менеджменту інформаційної безпеки та підсистеми попередження кризових ситуацій є актуальним завданням.

Метою роботи є розробка проектів, концептуальних документів у рамках побудови системи менеджменту інформаційної безпеки та розробка підсистеми попередження кризових ситуацій для підвищення рівня ІБ міжнародного аеропорту.

Основою забезпечення інформаційної безпеки сучасного міжнародного аеропорту є система менеджменту інформаційною безпекою, робота якої спрямована на захист інформаційних активів, забезпечення безперервної діяльності аеропорту, мінімізації ризиків інформаційної безпеки, виявлення вразливостей, забезпечення сталого розвитку і захищеності людей і матеріальних активів. Під контролем СМІБ стан інформаційної безпеки досягається після низки заходів таких як аудит інформаційної системи аеропорту, аудит ІБ, аудит вразливостей та потенційних загроз, розробка нормативних документів, політики безпеки та впровадження методів захисту інформації в усіх підрозділах аеропорту.

В ході виконання роботи було розкриті питання особливості забезпечення інформаційної безпеки міжнародного аеропорту, а також наведені рекомендації щодо створення надійної СМІБ та розроблені рекомендації щодо управління ризиками інформаційної безпеки міжнародного аеропорту. Актуальність цього питання сформовано тим, що аеропортам необхідно впроваджувати системи захисту від кіберзагроз, проте стандартизованих рекомендацій щодо впровадження подібних систем не розроблено.

Розроблено концептуальні проекти документів в рамках створення СМІБ міжнародного аеропорту (політика інформаційної безпеки, посадові інструкції персоналу з ІБ, концепції та програми реалізації ІБ, управління ризиками та системи оцінки управління ризиками), а також наведені рекомендації щодо створення надійної СМІБ, що відповідатиме стандартам ISO 27001 та ISO 27002.

Розроблено алгоритм та програмний засіб попередження кризових ситуацій, що надали можливість автоматизувати процес прогнозування кризових ситуацій та видача звіту по потенційним загрозам, що дало можливість підвищити ефективність виявлення загроз безпеці аеропорту.

Науковий керівник — д.т.н. Володимир Бурячок

Система виявлення аномалій для хмарних обчислень

УДК 004.056(043.2)
Валерій Журавель
Національний авіаційний університет, Україна, levaruz@ukr.net

На сьогодні тема хмарних обчислень є однією із найпопулярніших в дослідженнях і дискусіях IT-спеціалістів. Принцип організації хмарних систем є таким, що існуюча теоретична і практична база виявлення атак в ІС має певні обмеження щодо можливості їх ідентифікації в середовищі хмарних обчислень. Тому використання апарату нечітких множин для побудови системи виявлення аномалій, породжених атакуючими діями, є актуальною задачею, що дозволить вдосконалити існуючі системи виявлення вторгнень.

Метою роботи є розробка системи виявлення аномалій для хмарних обчислень. Новизною роботи є використання логіко-лінгвістичного підходу до побудови систем виявлення аномалій, що дасть змогу ефективно виявляти вторгнення в систему у реальному часі.

Під час виконання роботи було розглянуто основні поняття хмарних обчислень, їх природу та вразливості, які для них характерні, що дозволило використати отримані знання при побудові системи виявлення аномалій.

В результаті дослідження на основі моделі параметрів, універсальної моделі еталонів і моделі евристичних правил розроблено систему виявлення аномалій, яка дозволяє будувати засоби ідентифікації несигнатурних і нових атак за допомогою сформованих в нечітко визначеному слабоформалізованому середовищі параметрів.

Алгоритм роботи системи виявлення аномалій досить простий. Система отримує на вхід визначені параметри для певних видів аномалій (в нашому випадку зчитує ці дані з файлу логів), після цього проходить фазифікація параметрів, тобто відповідно до їх числових значень, їм присвоюється певний лінгвістичний терм, враховуючи множину еталонних нечітких чисел для кожного з параметрів. Даний набір термів складає логіко-лінгвістичну зв'язку, яка є актуальною для системи в даний період. Ця зв'язка порівнюється із евристичними правилами, які задають експерти і у випадку співпадіння, системі присвоюється в поточний період той рівень наявності аномалії, який поставлений у відповідність до тотожного правила.

Розроблено тестовий програмний засіб для дослідження запропонованої системи виявлення аномалій. Проведені дослідження показали, що система виявлення аномалій працює коректно. В результаті моделювання експерименту: під час подання на вхід системи лог-файлу із параметрами нормальної роботи системи, переважний рівень аномалії був "Низький", що доводить, що даний метод не дає сигналів фальшивої тривоги; під час подання на вхід файлу логів із параметрами, що моделюють роботу ботнета, система переважно визначала рівень аномалії як "вище середнього" та "високий", що дозволяє виявити відповідну аномалію.

Науковий керівник — к.т.н. Євгенія Іванченко

Система менеджменту інформаційної безпеки товариства з обмеженою відповідальністю «Консалтінг ЛТД»

УДК 004.056(043.2)

Андрій Заєць
Національний авіаційний університет, Україна, Zayots@bigmir.net

У зв'язку зі збільшенням обсягу інформації з обмеженим доступом, що циркулює в обчислювальних мережах і розширенням спектра завдань, які вирішуються за допомогою інформаційних систем, виникає проблема, пов'язана із зростанням числа загроз і підвищенням уразливості ресурсів. Тим самим виникає потреба у захисті інформації. Тому розробка та впровадження СМІБ для організації в теперішній час розвитку телекомунікаційних систем є актуальним.

Метою роботи є розробка системи менеджменту інформаційної безпеки для ТОВ «Консалтінг ЛТД». Новизна полягає у розробці методики, яка дозволить мінімізувати втрати критично важливих ресурсів організації, втрата яких може призвести до краху інформаційної системи, фінансового становища та репутації компанії.

Було проведено аналіз існуючої інфраструктури і заходів безпеки ТОВ, та зроблено висновок, що до моменту впровадження СМІБ рівень захищеності з точки зору документарних ризиків, становив 5,85%. Даний результат дає чітко зрозуміти, що при виникненні форс-мажорних обставин, Компанія зазнала б значних фінансових та репутаційних втрат, які б відобразились на позиціях Компанії на ринку України. Розроблено методику короткого опису критичних бізнес-процесів та методику аналізу та оцінки ризиків інформаційної безпеки на основі нормативно-правових актів України та національних стандартів. Розроблено алгоритм, який чітко відображає послідовність дій необхідних для якісного формування звіту за оцінкою ризиків інформаційної безпеки. За допомогою розроблених методик, було проведено аналіз та оцінку ризиків інформаційної безпеки, який відобразив, що захищеність інформаційного середовища Компанії незадовільний. На основі проведеної оцінки та аналізу було сформульовані рекомендації, щодо усунення ризиків інформаційної безпеки, які в свою чергу були доведені до відома керівництва Компанії для подальшої розробки плану заходів по керування ризиками інформаційної безпеки. На основі проведеного аналізу було сформовано та затверджено керівництвом Компанії, перелік нормативних документів, що потребують розробки для ефективного функціонування СМІБ. Було розроблено всі необхідні документи, тим самим мінімізувавши або усунувши більшість ризиків інформаційної безпеки. Програмно-апаратні ризики, які не були усунуті або мінімізовані за допомогою розробленої нормативної документації вимагають від керівництва Компанії значних фінансових та трудових інвестицій для їх усунення. Управління цими ризиками в свою чергу потребує значного проміжку часу, але згідно з розробленою СМІБ ці ризики можливо усунути в майбутньому. Незважаючи на залишкові ризики, можливо впевнено стверджувати, що рівень захищеності Компанії виріс у 5 разів.

Науковий керівник — к.т.н. Микола Тимошенко

Криптографічний модуль захисту даних з обмеженим доступом

УДК 004.056
Павло Добрянський
Національний авіаційний університет, Україна, dobryanski@gmail.com

На сьогоднішній день захист інформації стає усе більш актуальною і більш складною проблемою. Одним із можливих способів захисту при її передачі та зберіганні є криптографічний захист. На даний момент існує велика кількість криптосистем та алгоритмів захисту інформації, проте практично всі вони не досконалі − або повільні, або не забезпечують належної стійкості чи мають підмножини слабких ключів. Тому розробка нових більш ефективних систем та алгоритмів шифрування є актуальною задачею. Метою роботи є підвищення ефективності криптографічної обробки інформації шляхом розробки криптографічного модуля на основі удосконаленого методу шифрування інформації та розробленого методу генерації криптографічних ключів. Новизна роботи полягає в тому, що криптографічна система, яка за рахунок удосконалення методу захисту інформації, а саме ускладненням процедур обрахунку та операцій динамічного-циклічного зсуву дозволяє підвищити ефективність криптографічної обробки даних.

Аналіз методів захисту інформації показав, що багато завдань захисту інформації найефективніше вирішуються криптографічними методами, а ряд завдань взагалі може бути вирішений лише з використанням криптографічних методів захисту інформації. Дослідження існуючих симетричних систем шифрування даних та сучасних генераторів псевдовипадкових чисел дозволило вивчити їх структуру для можливого використання при удосконаленні алгоритму RC6 та розробці генератора криптографічних ключів. В результаті чого було розроблено метод генерації криптографічних ключів, що дозволило динамічно керувати процесом розсіювання інформації та удосконалено метод захисту інформації на основі алгоритму RC6 для підвищення швидкості криптографічної обробки даних та криптостійкості алгоритму. Розроблений програмний модуль заснований на основі удосконаленого симетричного алгоритму шифрування RC6, а саме з використанням ускладннених процедур обрахунку U і T. У даних процедурах пропонується ввести блок підстановок, операцію додавання за модулем 232 і множення за модулем 232, що забезпечить захист від алгебраїчних атак, лінійного та диференціального криптоаналізу, інтерполяційної атаки. Також пропонується ввести операції динамічного-циклічного зсуву (залежить від розширених ключів)– це дозволить динамічно керувати процесом розсіювання інформаційних даних. Розроблений криптомодуль характеризується найбільш високою швидкістю шифрування, і забезпечує як конфіденційність і достовірність, так і цілісність інформації, що передається.

Проведено експериментальне дослідження розробленого засобу захисту інформації, що підтвердило криптостійкість удосконаленого алгоритму до лінійного та диференціального криптоаналізу та дозволило визначити, що швидкість криптографічної обробки даних удосконаленим методом на 18.7 % вище, а розробленим генератором на 10.81 % вище ніж швидкість оригіналів.

Науковий керівник — д.т.н. Володимир Хорошко

Комплексна система захисту інформації автоматизованої системи класу 2 приватного підприємства

УДК 004.056
Владислав Скоріков
Національний авіаційний університет, Україна, vad18@bigmir.net

В теперішній час в провідних країнах світу склалася достатньо чітка система концептуальних поглядів на проблеми забезпечення інформаційної безпеки. Але, як свідчить реальність, кількість зловмисних дій над інформацією не тільки не зменшуються, а навпаки, має місце стабільна тенденція до її зростання. Для вирішення задач захисту інформації в організаціях створюється комплексна система захисту інформації (КСЗІ). Захист автоматизованої системи (АС) є найважливішою складовою КСЗІ, оскільки переважна частина інформаційних ресурсів присутня в електронному вигляді. КСЗІ організації є сукупністю методів та засобів об'єднаних єдиним цільовим призначенням та забезпечуючих необхідну ефективність захисту інформації організації. Створення системи захисту для відділу кадрів є необхідним, адже ця установа обробляє великий об'єм конфіденційних данних, в своїй більшості це є персональні данні, захист яких є обов'яковим за вимогами законодавства. Згідно вимог Закону України «Про захист персональних даних» метою роботи є побудова КСЗІ АС класу 2 приватного підприємства. Для визначення доцільності створення КСЗІ та зону її охоплення проведений аналіз, що включає в себе: виявлення конфіденційної інформації; Аналіз загроз та вразливостей. Згідно результатів проведеного аналізу – найвразливішим місцем в безпеці АС виявилася передача даних через мережу приватного підприємства у відкритому вигляді по незахищеному каналу. Тому велика частина роботи приділена створенню програмного комплексу, націленого на забезпечення конфіденційності та цілісності інформації, яка передається між клієнтськими та серверними частинами прикладних програмних систем відділу кадрів та забезпечує захист TCP-з'єднань з використанням механізмів та засобів криптографічного захисту інформації. Для створення КСЗІ на підприємстві було проведено ряд заходів. 1. Стартовий (Початковий): Отримання згоди вищого керівництва на створення КСЗІ; Розробка плану робіт з створенню КСЗІ. 2. Етап передпроектного обстеження. На цьому етапі проводилось обстеження (аудит) підприємства. 3. Проектування: створення системного проекту; створення «Політики безпеки» и т.д. 4. Впровадження. На цьому етапі проводилися всі пусконалагоджувальні роботи. Після реалізації цього етапу впроваджена КСЗІ готова до подальшого випробуванню. По результату випробування КСЗІ складений висновок щодо можливості представлення КСЗІ на державну експертизу. Розроблена КСЗІ АС класу 2 відділу кадрів приватного підприємства запобігає викраденню фінансових та матеріально технічних засобів; знищення майна та цінностей; розголошення та витоку персональної інформації; порушення роботи технічних засобів необхідних для забезпечення продуктивної діяльності відділу, включаючи інформаційні технології, що здійснюється за допомогою організаційних заходів та технічних методів захисту інформації. *Науковий керівник — к.т.н. Анатолій Давиденко*

Модуль захисту інформаційних потоків на базі електронного цифрового підпису

УДК 004.056

Павло Берлінець
Національний авіаційний університет, Україна, berlinetspavel@gmail.com

У світі електронних документів підписання документа за допомогою графічних символів втрачає сенс, тому що підробити і скопіювати графічний символ можна нескінченну кількість разів. Електронний цифровий підпис (надалі – ЕЦП) є повним електронним аналогом звичайного підпису на папері, але реалізується не за допомогою графічних зображень, а за допомогою математичних перетворень над вмістом документа. Особливості математичного алгоритму створення й перевірки ЕЦП гарантують неможливість підробки такого підпису сторонніми особами, що забезпечує властивість невідмовності від авторства. Надійність і зручність використання ЕЦП не викликає сумнівів. ЕЦП дає інформацію не тільки про особу, що підписала документ (автентичність повідомлення), але і дозволяє впевнитися, що сам документ не був змінений або підроблений після підписання (цілісність документа). Також одним з опціональних компонентів ЕЦП є позначка часу, яка показує реальний час підписання документа на відміну від дати, зазначеної в самому документі.

В даній роботі було проаналізовано низку алгоритмів ЕЦП, що використовуються на практиці та тих, що є основоположними в цій галузі. Усі ці алгоритми можуть бути класифіковані за проблемою, на якій засновані: проблеми факторизації великих простих чисел та проблеми дискретного логарифмування. Для використання в галузі криптографії є доцільним підбір такої групи чисел, де ці проблеми є важкорозв'язними, тобто відсутні субекспоненціальні алгоритми її вирішення. Було зазначено, що для проблеми факторизації таких груп поки що знайдено не було, в той час для дискретного логарифмування є альтернатива до груп вичетів за простим модулем – групи точок еліптичної кривої, що дозволяють досягти аналогічних показників безпеки при використанні ключів меншої довжини (224 біт проти 2048 для традиційних схем (DSA, ElGamal тощо)).

Метою роботи є - поєднання в створюваному методі ЕЦП переваг ефективності криптографічних схем, побудованих на арифметиці еліптичних кривих, з функціональністю RSA-подібних схем по відновленню підписаного повідомлення.

Наукова новизна полягає в наступному: розроблено новий метод ЕЦП, що заснований на алгоритмі підпису Шнорра, який дозволяє відновлювати дані безпосередньо з самого підпису аналогічно до RSA-подібних систем підпису. Розроблений метод дістав назву Elliptic Curve Digital Signature with Message Recovering (ECDSMR), що з англ. означає цифровий підпис на еліптичних кривих з відновленням повідомлення.

Науковий керівник – д.т.н. Володимир Хорошко

Програмний модуль оцінки ризиків інформаційної безпеки

УДК 004.056
Ярослав Ленько
Національний авіаційний університет, Україна, Lenko21@ukr.net

У сфері управління ризиками інформаційної безпеки залишаються деякі завдання, вирішення яких має важливе наукове та практичне значення. З цих позицій розробка і дослідження методів та засобів, які дозволяють створювати більш гнучкі у використанні інструменти для аналізу оцінювання ризиків втрат інформаційних ресурсів, вирішувати відповідні завдання, як на основі статистичних даних, так і на експертних оцінках, зроблених в невизначеному, слабоформалізованому середовищі є актуальним завданням.

Метою роботи є розробка програмного модуля оцінки ризиків інформаційної безпеки, що здатен працювати в умовах невизначеності. Новизною є використання теорії нечіткості під час процесу аналізу та оцінки ризиків, що дасть можливість оцінити стан системи без накопичування статистичних даних.

В роботі проведено дослідження основних завдань аналізу інформаційних ризиків та управління ними при організації режиму інформаційної безпеки та розглянуто міжнародну концепцію забезпечення інформаційної безпеки, а також різні підходи та рекомендації щодо вирішення завдань аналізу ризиків та управління ними. Подано огляд основних стандартів у галузі захисту інформації та управління ризиками: ISO 17799, ISO 15408, BSI, NIST, MITRE.

Проведено класифікацію понять ризик, управління ризиками, аналіз та оцінка ризиків; проведено порівняння існуючих методів та систем аналізу та оцінки ризиків та виявлено їх недоліки. На основі проведеного аналізу існуючих систем та методів аналізу та оцінки ризиків та використовуючи кортеж інтегральних параметрів ризику розроблено модуль аналізу та оцінки ризиків інформаційної безпеки, що здатен функціонувати в умовах нечіткості. Розроблено алгоритм та програмне забезпечення з використанням модулів обробки даних, нечіткого аналізу та генерації звітів, на основі яких реалізовано, побудовано та досліджено модуль аналізу та оцінки ризиків. Програмний модуль оцінки ризиків складається з наступних елементів: база даних загроз; база даних активів; блок формування ключових даних; блок оцінки значень оціночних компонентів; блок бінарної класифікації; блок оцінки значень ступенів ризику; лінгвістичне розпізнавання; блок ініціалізації ідентифікуючих компонентів; блок генерації звітів. Дослідження роботи модуля було проведено шляхом багатократного аналізу та оцінки ризиків для вибраних активів за умови постійних змін значень вхідних параметрів, що дає змогу припустити ефективність використання даного модуля для вчасного відслідковування позитивних і негативних змін в інформаційній безпеці організації, в умовах нечіткості та відсутності статистичних даних про інциденти. Отже, на основі використання лінгвістичних змінних, розроблено програмне забезпечення аналізу і оцінки ризиків, яке може не використовувати статистичні дані та здатне працювати в умовах невизначеності.

Науковий керівник — к.т.н. Сергій Карпенко

Програмний модуль оцінки безпеки інформаційних ресурсів у мережах передачі даних

УДК 004.56.5(043.2)
Олександр Панасюк
Національний авіаційний університет, Україна, camelne.hd@gmail.com

Велика кількість електронних злочинів пов'язана із несанкціонованим доступом до інформаційних ресурсів комп'ютерних систем (КС), які працюють в режимі реального часу. Такі системи керують банкоматами та платіжними терміналами, їх власники змушені звертатися до експертів, які проводять аудиторську перевірку безпеки інформаційних ресурсів (ІР) КС.

Найбільш надійний захист інформації в КС можна забезпечити тільки за допомогою системного підходу. Він припускає, що рішення задачі повинне досягатися за рахунок використання сукупності організаційних і організаційно-технічних мір і заходів, а також криптографічних систем і засобів. Один з етапів побудови такої системи передбачає аналіз та оцінювання загроз таким ресурсам. Чітка система класифікації загроз допоможе експерту розробити ефективні рекомендації по підвищенню рівня захищеності ІР. Тому на сьогодні питання вибору засобів оцінювання залишаться досить актуальним.

Виходячи з цього, метою даної роботи є побудова модуля оцінювання безпеки ІР, які циркулюють у мережах передачі даних.

Для досягнення поставленої мети було вирішено низьку задач, а саме: проведений аналіз існуючих підходів і програмних систем оцінювання безпеки ІР в КС; на основі отриманих результатів розроблений модуль аналізу та оцінювання безпеки ІР у мережах передачі даних; проведене експериментальне дослідження розробленого програмного модуля, яке показало, що зі зміною середовища оцінювання з детермінованого на слабоформалізоване, нечітке, результати змінюються адекватно.

Аналіз стандартів для проведення аудиту показав, що всі вони містять лише загальні рекомендації, які повинен виконати експерт при проведенні аудиту ІР КС. Таким чином, при використанні сучасної методичної бази, оцінка ефективності засобів захисту інформації носить нечіткий, суб'єктивний характер; практично повністю відсутні нормовані кількісні показники, що враховують можливі випадкові або навмисні дії.

В роботі було запропоновано програмний модуль, який дозволяє проводити експерту оцінювання у різних середовищах, а також при нечітко заданих параметрах, з використанням нечіткого математичного апарату.

Таким чином, проведення аналізу та оцінки загроз безпеки ІР за допомогою представленого програмного модуля, дозволить підвищити рівень захищеності інформаційних ресурсів КС, які працюють в режимі реального часу.

Науковий керівник — к.т.н. Світлана Казмірчук

Системи цілісності web-сайту товариства з обмеженою відповідальністю

УДК 004.056.5 (043.2)

Тетяна Панівко
Національний авіаційний університет, Україна, tasha_sdi@ukr.net

Публічні web-сайти продовжують залишатися об'єктами атак хакерів, які хочуть за допомогою цих атак нанести втрату репутації організації або добитися яких-небудь політичних цілей. Хороші заходи захисту можуть захистити сайт від тих неприємностей, які матиме організація у разі успішної атаки на нього. Можливий різний збиток – від простого блокування роботи сервера до заміни його вмісту порнографічним матеріалом, політичними гаслами або видалення груп файлів, а також розміщення на сервері програм-троянських коней. У зв'язку з цим гарантування цілісності вмісту публічного web-сайту компаній є актуальною задачею.

Метою роботи є підвищення рівня безпеки web-сайту товариства з обмеженою відповідальністю від атак зловмисників, шляхом забезпечення його цілісності.

Для досягнення поставленої мети, було: проведено аналіз існуючих атак, які направлені на порушення цілісності вмісту web-сайту та методи захисту від них; на підставі отриманих результатів аналізу, розроблено структурне рішення системи захисту цілісності web-сайту товариства з обмеженою відповідальністю; реалізовано програмний застосунок представленої системи; проведено експериментальне дослідження програмного забезпечення.

Представлена система забезпечення цілісності web-сайту складається з декількох модулів, зокрема: формування та збереження еталонів, генерації цифрового підпису, перевірки цифрового підпису, відновлення.

Робота системи починається зі формування та збереження у демілітаризованій зоні еталонної копії та цифрового підпису web-сайту. Через визначений проміжок часу генерується цифровий підпис самого web-сайту та модулем перевірки цифрового підпису отриманий результат порівнюється з еталонним значенням. Якщо значення цифрового підпису не співпадає, відбувається відновлення вмісту web-сайту за допомогою відповідного модуля. Система працює у напівавтоматичному режимі. Адміністратор безпеки повинен ініціювати запуск та перезапуск системи при кожній зміні його вмісту.

Запропонована система захисту цілісності вмісту web-сайту товариства з обмеженою відповідальністю, дала змогу підвищити рівень захищеності сайту та гарантувати швидке відновлення його під час реалізації DoS та DDoS атак на нього.

Ця система може бути використана під час реалізації, як комплексних систем захисту інформації web-сервесів у вигляді окремої підсистеми, так і для забезпечення тільки цілісності їх, як повноцінна система.

Науковий керівник – к.т.н. Світлана Казмірчук

Модуль аутентифікації та доступу до інформаційних ресурсів автоматизованих систем

УДК 004.056.53 (043.2)
Дмитро Абраменко
Національний авіаційний університет, Україна, faith13@ukr.net

Робота присвячена вирішенню питання автентифікації та контролю доступу до інформаційних ресурсів АС. Дане питання є актуальним в сучасному суспільстві та досить активно досліджується.

В роботі розглянуті основні нормативні документи щодо захисту інформації в автоматизованих системах. Також в роботі приведено основні загрози інформаційній безпеці в автоматизованій системі класу 3, а також розроблено модель порушника. В роботі наводиться загальна структурна схема автоматизованої системи класу 3, в якій вказано її основні структурні компоненти. Проведено поділ суб'єктів автоматизованої системи на ієрархічні групи відповідно до функціональних обов'язків та повноважень. Було створено таку систему суб'єктів, яка є універсальним відображенням системи взаємодії працівників довільної організації та може використовуватись, як еталон при розробці політики безпеки на практиці в реальних виробничих умовах. Було виділено групу керівництва, окремо адміністратора та адміністратора безпеки, керівників підрозділів або робочих груп, а також співробітників, що входять до цих робочих груп. При чому, функціональні обов'язки, що покладаються на робочі групи відрізняються, тому повноваження співробітників різних груп, а відповідно і створені ролі також відрізняються. В роботі проведено аналіз існуючих методів та схем автентифікації. На практиці було розроблено та реалізовано метод автентифікації та контролю доступу до інформаційних ресурсів автоматизованої системи. Було розроблено математичну модель методу автентифікації. Розроблений метод може використовуватися в автоматизованих системах класу 3. Загальні принципи розробленого методу є досить універсальними і їх можна використовувати не лише для забезпечення інформаційної безпеки автоматизованих систем класу 3, а й для автоматизованих систем класу 2, додавши кілька додаткових рубежів захисту, що враховують специфіку та особливості даного класу автоматизованих систем. Розроблений метод автентифікації детально описаний у формальному вигляді та проілюстрована саналітичною моделлю. В ході проведення даного дослідження було вирішено ряд задач: досліджено та визначено основні закономірності функціонування, обробки та передачі інформації в автоматизованих системах загалом та автоматизованій системі класу «3»; досліджено та проведено аналіз сучасних методів аутентифікації та контролю доступу та різноманітних алгоритмів, що покладені в основу цих методів; виявлено слабкі та сильні сторони та проведено порівняльноий аналіз цих алгоритмів; розроблено та реалізовано метод автентифікації та контролю доступу. Новизною даної роботи є розроблений метод аутентифікації та контролю доступу до інформаційних ресурсів автоматизованої системи класу «3». *Науковий керівник – д.т.н. Володимир Хорошко*

Програмний застосунок захисту конфіденційних даних

УДК 004.056
Тетяна Старовойт
Національний авіаційний університет, Україна, starovoit_tania@mail.ru

На сьогодні в Україні системи накопичення і обробки інформації та реалізація доступу до них з використанням мережних технологій швидко розвиваються і комерціалізуються. Процеси масового споживання інформаційних ресурсів потребують особливих підходів до їх організації та розвитку. Відповідність змісту інформації, що поставляється, задачам користувачів, її повнота, своєчасність, форма подання є критеріями корисності інформаційного забезпечення, за ними судять, наскільки успішною є науково-інформаційна діяльність інформаційних ресурсів. Особливо актуальним питанням є захист інформації конфіденційного характеру та підвищення оперативності доступу до конфіденційних інформаційних ресурсів в комп'ютерних системах.

Метою розв'язання цієї проблеми – є вирішення важливої науково-технічної задачі підвищення швидкодії доступу до конфіденційних інформаційних ресурсів на основі використання логічних функцій для криптографічного перетворення в комп'ютерних системах.

Аналіз існуючих методів та засобів криптографічного захисту інформації дав змогу визначити основні підходи забезпечення підвищення оперативності доступу до конфіденційних інформаційних ресурсів. З урахуванням визначених підходів було обрано та описано методи, які використані в швидкодіючій системі доступу до конфіденційних даних, а саме математичні моделі логічних функцій перекодування, які можуть бути покладені в основу реалізації пристроїв криптографічного перетворення інформації з метою застосування метод підвищення швидкодії доступу до інформації в системах захисту інформації на основі логічних функцій та приведено алгоритм методу підвищення швидкодії доступу до конфіденційних інформаційних ресурсів, в основу якого було покладено метод підвищення швидкодії систем захисту інформації на основі спеціалізованих логічних функцій. В основу розробки системи перекодування інформації покладено метод підвищення оперативності доступу до конфіденційних інформаційних ресурсів на основі використання логічних функцій для криптографічного перетворення шляхом введення логічних функцій перекодування, що дозволило зменшити час доступу до інформації за рахунок заміни процесу «декодування-кодування».

Результатом виконаної роботи є програмна система доступу до конфіденційних даних на основі використання логічних функцій для криптографічного перетворення інформації на основі логічних функцій за рахунок розробки математичних моделей та функціональних схем побудови функцій перекодування, що дало змогу розробити систему підвищення оперативності доступу до віддаленої захищеної інформації в реальному часі. Застосування розробленого програмного застосунку дозволяє підвищити оперативність доступу до конфіденційної інформації від 1,65 до 3,1 разів залежно від часу отримання ключа та розрядності перетворення.

Науковий керівник – к.т.н Василь Бриль

Програмний модуль захисту від атак на основі онлайн-пасток

УДК 004.056
Михайло Сікіріцький
Національний авіаційний університет, Україна, sikiritckyy@nau.edu.ua

На сьогодні особливо гострим є питання виявлення та протидії найновішим, ще невідомим типам та методам злому, вірусам, шкідливому програмному забезпеченню та іншій зловмисній діяльності, які відомі під загальною назвою «0-day-атаки». Виходячи із вище сказаного актуальним є питання вдосконалення практичних засад побудови та функціонування систем приманок із забезпеченням прихованого та комплексного контролю процесу злому для оперативного реагування на нові та невідомі атаки.

Метою роботи є створення не дорогого та легкого у реалізації програмного модуля захисту від атак на основі Honeypot за рахунок адаптивного і проактивного захисту інформаційного ресурсу на базі моделі Honeypot та захисту від DoS- та DDoS-атак.

Новизна є в удосконаленні системи захисту від атак на основі Honeypot за рахунок модуля адаптивного та проактивного захисту, що дозволить приховати від зловмисника процес стеження та аналізу його дій і оперативно реагувати на нові та невідомі атаки.

При створенні програмного модуля були враховані наступні чинники. Розроблений засіб повинен бути легкий в модернізації та налаштуванні, мати відкритий вихідний код та детальну документацію, можливість самостійної модернізації та інтегрувння в комплекс Honeypot на базі User Mode Linux.

Проведений аналіз методів проектування Honeypot та її віртуалізації на базі User Mode Linux, дозволив вибрати найбільш підходяще програмне забезпечення та дозволив створити систему захисту яка відповідає усім вимогам спеціаліста та підприємства. Розроблена архітектури та структури Honeypot з використанням User Mode Linux що дозволила створити та налаштувати комплекс Honeypot, котрий створює віртуальну копію локальної мережі підприємства, а також пов’язати та налаштувати тонку взаємодію програмного забезпечення. Для створення пастки було використовую HoneyD - це спеціалізована платформа для побудови пасток. Вона працює за модульним принципом. Кожен сервіс - окремий скрипт, що визначає поведінку пастки і реалізує механізм «запит-відповідь». Крім того, HoneyD має розширені засоби формування віртуальних мереж, в яких роль вузлів виконують сконфігуровані пастки.

Для спроектованої архітектури Honeypot було розроблено програмний модуль, який складається з двох основних компонентів: блоку перевірки трафіку та блоку аналізу дій користувача. Блок перевірки трафіку - це не тільки IDS (система виявлення вторгнень), але ще й IPS (система їх запобігання) і відповідно боротьби з DDoS атаками. Блок перевірки трафіку підтримує наступні інтерфейси для прослуховування: Ethernet, SLIP, PPP. Блок перевірки трафіку може працювати на багатьох операційних системах: Linux, Windows, IRIX, SunOS, * BSD та ін. Блок перевірки трафіку складається з сенсорної підсистеми, підсистеми аналізу та підсистема зберігання результатів

аналізу. Блок аналізу дій користувача грунтується на фільтрації пакетів, що проходять через з'єднання, і відповідно до набором правил визначає ту чи іншу реакцію брандмауера на ці пакети.

Розроблений програмний модуль може бути впроваджений на підриємстві як недорогий та ефективний засіб захисту від DoS- та DDoS-атак у порівнянні із комерційними аналогами.

Науковий керівник — к.т.н. Микола Тимошенко

Система підтримки проведення аудиту приватного підприємства

УДК 004.056(043.2)
Костянтин Непорожний
Національний авіаційний університет, Україна, e4d5ed@gmail.com

Управління ІБ стає все більш значущим для приватних компаній в міру їх зростання та виходу на міжнародні ринки. Тому розробка системи управління інформаційною безпекою (СУІБ) на підприємстві, яка б гарантувала партнерам функціонування компанії без помилок в роботі інформаційних систем є актуальним завданням.

Метою роботи є розробка системи підтримки проведення аудиту приватного підприємства згідно стандарту ISO/IEC 27001:2005. Новизною є застосування сучасного стандарту проведення аудиту для захисту власних інформаційних ресурсів, що дозволить ефективно вирішувати і попереджувати проблеми підприємства, які пов'язані з інформацією. Під час розробки системи, було проведено аналіз цілей та функцій роботи підприємства, а також робочих обов'язків кожного співробітника. Було виявлено, що у нормативно-правових актах, положеннях та інструкціях, які регламентують роботу підприємства відсутня інформація, що регламентує правила доступу до робочої інформації співробітниками. В процесі розробки було отримано такі практичні результати: побудовано схему життєвого циклу інформації на підприємстві; створено списки інформації, які дали можливість здійснити розмежування прав доступу до інформації між співробітниками; вдосконалено метод визначення повноважень шляхом створення уніфікованої системи, що базується на детальному аналізі нормативно-правових актів, внутрішніх інструкцій та постанов, які регламентують роботу кожного співробітника для забезпечення захисту інформації підприємства на базі розробленого додатку на мові C++. Проведено практичне дослідження створеної системи, результатом чого стало створення сучасних правил доступу та роботи із службовими інформаційними ресурсами для забезпечення їх захисту на приватному підприємстві. Основними завданнями, які вирішуються при використанні даної системи є визначення повноважень для забезпечення захисту інформації підприємства: розмежування доступу до службової інформації; аналіз потреб співробітників у інформації; підвищення захищеності службової інформації.

Розроблена система була протестована при експериментальному проведенні аудиту інформаційної безпеки на відповідність стандарту ISO 27001:2005 на приватному підприємстві «Будпроект», та отримала схвальні відгуки пра-

цівників інформаційно-обчислювального центру, що обули залучені до проведення аудиту, оскільки швидкість аудиту зросла в 6 разів, час інтеграції системи до сайту-носія – близько 10 хвилин, й це одноразова операція, в майбутньому запуск системи триватиме не більше 2 хвилин (в залежності від швидкості Інтернету), у той час як встановлення системи аудиту займає від 40 хвилин до 3 годин. Крім того інтерфейс даної системи підтримки аудиту максимально спрощений й інтуїтивно зрозумілий. Оригінальна анкета опитування персоналу та алгоритм аудиту дозволили підвищити результативність перевірки у порівнянні з раніше використовуваними системами. Також це все це привело до спрощення роботи аудитора.

Науковий керівник — к.т.н. Євгенія Іванченко

Система захисту програмного коду від несанкціонованого дослідження

УДК 004.056

Рафік Адиширінов
Національний авіаційний університет, Україна, Rk_054@mail.ru

У наш час захист комерційних версій програм звичайно зводиться до вбудовування фрагмента, що містить перевірку ключа, а для злому сучасних програм найчастіше використовують їх динамічний аналіз і за допомогою різних налагоджувачів визначають місце перевірки ключа. Як правило, досить легко виявити місце порівняння введеного ключа з «правильним» значенням і, модифікувавши код захищеної програми, домогтися її працездатності. Найбільш відомі методи захисту змінюють або блокують роботу налагоджувальних засобів. Таким чином, у відповідь на різні створювані засоби захисту хакери розробляють способи їхнього злому, тому необхідно постійно створювати нові підходи для вдосконалення методів захисту. Так, актуальність роботи обумовлена необхідністю розробки нових підходів для підвищення результативності захисту програмного забезпечення від прихованого сканування з метою забезпечення авторських прав розроблювачів програм, а також для запобігання загроз з боку шкідливих програм.

Метою роботи є розробка системи захисту програмного коду від прихованого сканування, а новизною є розробка моделі із застосуванням важкооборотних задач, що дасть можливість забезпечити експоненціальне зростання часу підбору ключа для реалізації поставленого завдання.

Пропонується використовувати важкооборотні задачі для захисту програм, а саме, розробляти захисний фрагмент таким чином, щоб при його побудові і/або при роботі із правильним ключем вирішувалася пряма задача, що вимагає поліноміального часу для свого розв'язку, а при зломі хакерові довелося б вирішувати зворотну *NP* -повну задачу. Запропонована загальна модель, що використовує важко оборотні задачі для захисту програм від несанкціонованого використання, заснована на вбудовуванні захисного фрагмента, заснованого на двох рівнях захисту. Перший рівень використовує властивість деяких комбінаторних завдань, що полягає в тому, що задачі, їм зворотні, вимагають для розв'язку більших обчислювальних витрат. При

вбудовуванні захисного фрагмента й при роботі легального користувача вирішується пряма задача, а зломщикові для одержання секретного ключа доводиться вирішувати зворотну важковирішуєму задачу. Другий рівень захисту спрямований на захист від налагодження, при цьому захисні фрагменти, що вбудовуються, максимально «затемнюють» місце перевірки ключа й переходу на точку входу в програму, що захищається. При розробці моделі були дотримано три вимоги до формування засобів захисту: функціональна повнота, гнучкість і уніфікованість використання. На основі запропонованої моделі спроектовано систему захисту програмного забезпечення від прихованого сканування.

Особливістю розробленої системи є можливість розділити розв'язок задачі на паралельно працюючі потоки й у такий спосіб забезпечити нелінійність виконання коду програми, що робить вивчення її роботи нетривіальною задачею. Використовувана в реалізації багатопоточність дозволяє повністю деморалізувати хакера й блокує використання їм налагоджувальних засобів.

Науковий керівник — к.т.н. Євгенія Іванченко

Програмний застосунок адміністрування баз даних

УДК 004.056(043.2)

Євген Григор'єв
Національний авіаційний університет, Україна, grygoriev.evgeniy@gmail.com

Бази даних (БД) та системи управління ними широко використовуються в сучасних інформаційних технологіях. Бази даних є невід'ємною частиною інформаційних ресурсів будь-якого підприємства, в яких зберігають бухгалтерську і матеріальну звітність організації, дані працівників та ін. Значна частина інформації зберігається також у базах даних на web-сервері організації. Переважна більшість використовуваних БД відповідають реляційній моделі даних, проте є широке коло завдань, що вимагають використання надвеликих баз складноструктурованих даних, вимогам яких реляційні СУБД задовольняють не в повній мірі, що змушує розробників придивлятися до альтернатив реляційних баз даних. Сукупність таких технологій відома як «NoSQL бази даних», що дають розробникам високу швидкість внесення змін у додатки, низькі витрати на масштабування, інструменти обробки і зберігання великих обсягів даних, а також високу швидкість виконання на відносно недорогому обладнанні.

Актуальність роботи полягає в забезпеченні захищеності БД web -додатків, робота яких реалізована в середовищі NoSQL, а також в забезпеченні легкої горизонтальної масштабованості БД і підтримці відмовостійкості, реалізації ефективного зберігання двійкових даних великих обсягів.

Метою роботи розробка програмного застосунка адміністрування баз даних web–додатків. Новизна полягає у збільшенні швидкості роботи з великими об'ємами даних з БД і реалізації горизонтальної масштабованості web-додатків, за рахунок розробки спеціалізованої серверної системи

адміністрування даних в середовищі NoSQL на основі нереляційної БД MongoDB для баз даних з обмеженим доступом.

Аналіз існуючих реляційних СУБД і NoSQL методів збереження даних, показав, що для досягнення поставленої мети доцільно обрати документо-орієнтовану СУБД MongoDB. Використовувана модель зберігання даних (JSON / BSON) простіше кодується, простіше управляється, а внутрішнє угруповання релевантних даних забезпечує додатковий виграш в швидкодії. Нереляційний підхід досить зручний для створення баз даних, у яких горизонтальне масштабування має на увазі розгортання на безлічі машин.

Для коректного функціонування ДОСУБД MongoDB спочатку було проведено налаштування та модернізацію базового пакету локального web-серверу згідно вимог серверу ДОСУБД MongoDB. Після чого встановлено і запущено через консоль сервер самої БД. Розроблено алгоритми роботи системи адміністрування і структурну схему роботи, програмно налаштовано взаємодію інтерпретатора PHP з сервером ДОСКБД.

Результатом роботи є програмний інструмент адміністрування для MongoDB, документо-орієнтованої NoSQL СУБД, для баз даних з обмеженим доступом, що має відкритий вихідний програмний код, дозволяє адмініструвати кілька серверів і мати кілька записів адміністратора, має швидке переключення між хостами, і дозволяє створювати, додавати, видаляти, відновлювати і розробляти структуру NoSQL баз даних.

Науковий керівник — к.т.н. Євгенія Іванченко

Програмний застосунок захисту web-сервісу інтернет-провайдера

УДК 004.056

Максим Когут

Національний авіаційний університет, Україна, kogut_05@mail.ru

На сьогодні в Україні системи накопичення і обробки інформації та реалізація доступу до них з використанням мережних технологій швидко розвиваються і комерціалізуються. Процеси масового споживання інформаційних ресурсів потребують особливих підходів до їх організації та розвитку. Відповідність змісту інформації, що поставляється, задачам

користувачів, її повнота, своєчасність, форма подання є критеріями корисності інформаційного забезпечення, за ними судять, наскільки успішною є науково-інформаційна діяльність інформаційних ресурсів. Особливо актуальне питання постає про захист інформації конфіденційного характеру та підвищення оперативності доступу до конфіденційних інформаційних ресурсів в комп'ютерних системах.

Метою розв'язання цієї проблеми – є вирішення важливої науково-технічної задачі підвищення швидкодії доступу до конфіденційних інформаційних ресурсів на основі використання логічних функцій для криптографічного перетворення в комп'ютерних системах. Новизною роботи є підвищення швидкодії доступу до ресурсів інформаційних систем за рахунок

впровадження спеціалізованих логічних функцій, що дасть змогу підвищити оперативність доступу до конфіденційної інформації.

Аналіз існуючих методів та засобів криптографічного захисту інформації дав змогу визначити основні підходи забезпечення підвищення оперативності доступу до конфіденційних інформаційних ресурсів. З урахуванням визначених підходів було обрано та описано методи, які використані в швидкодіючій системі доступу до конфіденційних даних, а саме математичні моделі логічних функцій перекодування, які можуть бути покладені в основу реалізації пристроїв криптографічного перетворення інформації з метою застосування методу підвищення швидкодії доступу до інформації в системах захисту інформації на основі логічних функцій та приведено алгоритм методу підвищення швидкодії доступу до конфіденційних інформаційних ресурсів, в основу якого було покладено метод підвищення швидкодії систем захисту інформації на основі спеціалізованих логічних функцій.

В основу розробки системи перекодування інформації покладено метод підвищення оперативності доступу до конфіденційних інформаційних ресурсів на основі використання логічних функцій для криптографічного перетворення шляхом введення логічних функцій перекодування, що дозволило зменшити час доступу до інформації за рахунок заміни процесу «декодування-кодування».

Результатом виконаної роботи є програмна система доступу до конфіденційних даних на основі використання логічних функцій для криптографічного перетворення інформації на основі логічних функцій за рахунок розробки математичних моделей та функціональних схем побудови функцій перекодування, що дало змогу розробити систему підвищення оперативності доступу до віддаленої захищеної інформації в реальному часі. Застосування розробленого програмного застосунку дозволяє підвищити оперативність доступу до конфіденційної інформації від 1,65 до 3,1 разів залежно від часу отримання ключа та розрядності перетворення.

Науковий керівник — к.т.н. Микола Тимошенко

Стеганографічний програмний модуль для забезпечення конфіденційності даних

УДК 004.415.24

Захар Кириченко
Національний авіаційний університет, Україна, easygoingboy@ukr.net

Актуальність проблеми забезпечення інформаційної безпеки постійно зростає і стимулює пошук нових методів захисту інформації. Розвиток комп'ютерних методів обробки інформації дозволив істотно підвищити рівень інформаційної безпеки. Значних успіхів у цьому напрямку вдалося домогтися з використанням сучасних криптографічних методів. Аналіз існуючих систем захисту інформації показав, що на відміну від криптографічних систем захисту інформації сьогодні все більш популярними стають системи захисту інформації, що засновуються на стеганографічних методах та алгоритмах або

системи, що поєднують в собі, як криптографічні так і стеганографічні методи захисту інформації.

Метою роботи є розробка модуля забезпечення конфіденційних даних для передачі їх каналами загального користування. Новизною роботи є підвищення стійкості стеганографічного захисту інформації до атак пасивного й активного порушників у відкритих каналах зв'язку за рахунок комбінації криптографічних та стеганографічних методів.

У зв’язку з цим пропонується метод вбудовування цифрових даних, які попередньо зашифровані криптографічним алгоритмом, в аудіо-контейнер На основі запропонованого методу створена модель криптостеганосистеми захисту цифрових даних, яка дозволяє легко приховувати вихідне повідомлення в аудіо-контейнері, добувати приховане повідомлення з нього і при цьому залишалася стійкою до атак, як програмним пошуковими роботами і аналізаторами, так і уважному перегляді тексту людиною. Приховування інформації відбувається наступним чином. Мовний файл, який був раніше записаний та може містити довільний текст, як на українській, так і на іноземних мовах, за допомогою спеціальної програми-плагіна розпізнавання мови розподіляється на склади – сегментується. Наступний етап вбудовування раніше підготовленого повідомлення в звук-контейнер, при цьому вихідне повідомлення у нас буде шифруватися криптографічним алгоритмом RSA, задля підвищення рівня захищеності даних, що будуть передаватись. Процесом вбудовування інформації в контейнер буде займатися спеціалізована програма, яка відповідно до завчасно визначених рівнів тону буде змінювати ці рівні на незначні значення. Відповідно після проведення вказаних операцій ми отримаємо аудіофайл з вбудованим в нього зашифрованим повідомленням, яке складається з цифрових даних. Отримане повідомлення готове для передачі. Стенограма, яку отримав адресат порівнюється з оригіналом, знаходяться зміни – а саме склади в яких було змінено просодійні характеристики – рівні основного тону. Відповідно по цим змінам і буде знайдено наше вихідне повідомлення. За цим у нас слідує процес розшифрування повідомлення, адже воно було зашифровано алгоритмом RSA. В результаті ми отримуємо цифрові дані, які і є нашим вихідним повідомленням.

Варто також зазначити, що при використанні даного методу важливим є питання дезінформації зловмисника, або супротивника. Варто використовувати його при глобальній переписці між організаціями або людьми. Навіть у випадку коли зловмисник буде проводити аналіз трафіку він не зможе з усього потоку інформації виокремити саме необхідне повідомлення, бо його вигляд ні чим не буде відрізнятись від інших повідомлень – аудіо не змінює ні свого формату, ні інших показників.

Науковий керівник — к.т.н. Микола Тимошенко

Система аналізу попиту на ринку нерухомості в місті Києві

УДК 347.451.4:330.101.52(477-25)(043.2)
Ніна Кочетова
Національний авіаційний університет, Україна, ninon17@ukr.net

Аналіз ринку нерухомості є невід'ємною складовою системи економічних відносин, тісно пов'язаної з процесами, що відбуваються на ринках споживчих товарів, інвестиційних ресурсів, капіталу, цінних паперів, праці. Ринок нерухомості являє собою складну багатофакторну, саморегульовану та керовану соціально-економічну систему, яка суттєво впливає на фінансово-грошові потоки в економіці, напрями їх руху та рівень дохідності.

Актуальність теми. Розглядаючи досвід європейських країн можна відмітити те, що ринок нерухомості в Україні перебуває на початкових етапах формування, тому це зумовило затримку в науковому аналізі його основних закономірностей. Для сучасних умов функціонування перехідної економіки актуальним є аналіз ринку нерухомості, оскільки він є частиною виробничого потенціалу країни і може використовуватись в якості двигуна економічного зростання.

Метою є аналіз попиту і визначення тенденцій змін ринку нерухомості в м.Києві у середньому і довгостроковому періодах шляхом використання статистичних методів аналізу пакету прикладних програм «Логос». Предметом дослідження є система базового інформаційного та експертно-аналітичного програмно-технічного комплексу «Логос». Об'єктом дослідження виступає ринок нерухомості в м.Києві. Найбільш важливими сегментами ринку нерухомості України на сьогодні є ринки житлової нерухомості, комерційної нерухомості та ринки землі. Оскільки Київ є столицею України, одним з найбільших міст Європи з чисельністю населення 3 млн., який є політичним, історичним, соціально-економічним, транспортним центром, тому ринок нерухомості в ньому є насиченим та показовим відображенням перспектив розвитку економіки міста в цілому.

Для кожного з методів аналізу (а саме: метод групових середніх; метод класифікації; кластерно-спектральний аналіз) вхідними даними є таблиці цінових показників житлової та комерційної нерухомості в м.Києві. В результаті обробки вхідних даних за допомогою алгоритмів вище зазначених математико-статистичних методів на виході отримаємо сукупність числової, текстової та графічної інформації, яка з бази даних перетворилась в знання.

Отже, проаналізувавши динаміку попиту на ринку нерухомості можна зробити висновки про тенденції в економіці: спад попиту на ринку нерухомості передує спаду економіки загалом, а підйом настає, як правило, раніше, ніж в економіці.

Науковий керівник — к.т.н. Василь Бриль

Побудова прогнозу розвитку регіону в умовах «трансформаційного» періоду

УДК 332.1.012.2.001.18(045)
Василь Бриль, Олександр Суліма
Національний авіаційний університет, Україна,
vamibr@ukr.net, openssl@inbox.ru

В умовах різкої зміни геополітичної ситуації недостатньо простих методів екстраполяції для побудови прогнозу розвитку регіону. У той же час через нестабільності різко зростає ціна помилки при прогнозуванні. Пропонується провести порівняльний аналіз методів прогнозування екстраполяцією, прогнозування пасивним розподілом ресурсів та прогнозування побудованими нейромережами в сучасних умовах. Використовуючи раніше побудовані моделі на основі даних ВВП, сукупного внутрішнього попиту, ВРП регіону.

Для аналізу будуть використані напрацювання отримані при проходженні практики в інформаційно-аналітичному центрі ЕКСОР, використовуючи програмне забезпечення ЛОГОС. Загальна технологія прогнозування складається з наступних етапів: аналіз об'єкту прогнозування; вибір прогнозованого показника і факторів, які впливають на його рівень; вибір методів, які пов'язують фактори і об'єкт прогнозування або побудова моделі, яка відображає логічну і статистичну адекватність об'єкту; збір статистичних даних і наповнення абстрактної економічної моделі (системи рівнянь) необхідними статистичними даними; проведення прогнозних (експертних) розрахунків на основі відібраних методів чи моделі; оцінка якості та вірогідності прогнозу; опис результатів прогнозування і рекомендації для формування управлінських рішень.

В якості прикладу спробуємо проаналізувати схожість (відмінність) підприємств-експортерів за їх фінансово-економічними показниками (у розрізі галузей промисловості), використовуючи кластерно-спектральний аналіз. Для вхідних змінних було обрано (рис. 1) таблицю галузі промисловості.

Галузі промисловості - показники: таблиця бази даних

	Key	Галузь	Обсяги	Обсяги	Інвестицій	Рентабел
	1	Виробн...	1,58	1,75	1,8	1,8
	2	Целюло...	0,67	1,17	0,8	1,17
	3	Виробн...	1,28	0,97	1,9	0,97
	4	Лісова и...	1,24	1,6	0,86	0,69
	5	Виробн...	1,07	0,89	0,93	0,56
	6	Видобув...	1,1	0,84	0,81	0,62
	7	Агропро...	0,98	0,69	1,2	0,71
	8	Трансп...	1	0,73	0,82	0,73
	9	Послуги	1,15	0,44	0,74	1,7

Рис. 1. Таблиця вхідних даних для дослідження підприємств різних галузей промисловості (кластерно-спектральний аналіз)

Для фінансово-економічних показників використані позначення: обсяги реалізації; обсяги експорту; інвестиційна привабливість; рентабельність. Графічне зображення (рис. 2) результату розрахунку методу має вигляд.

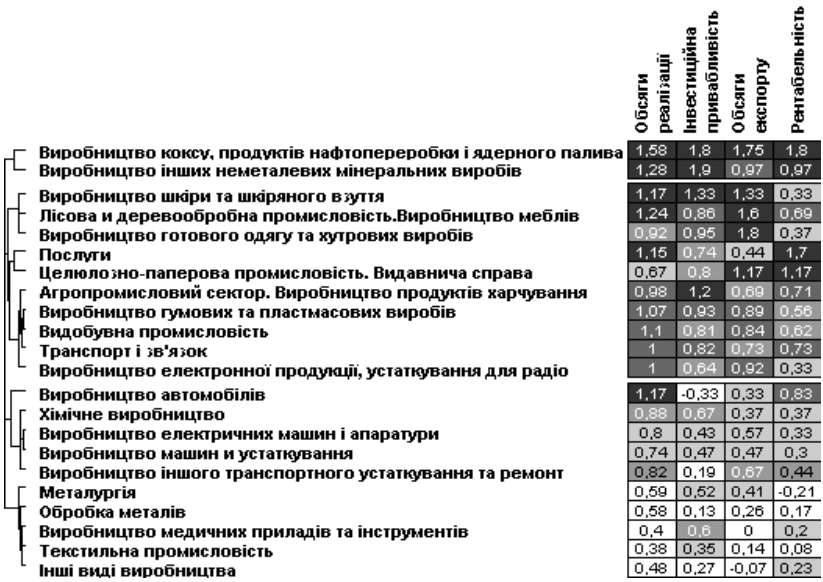

Рис. 2. Кластерно-спектральна карта – дослідження підприємств різних галузей за їх фінансово-економічними показниками

Середні експертні оцінки, що характеризують фінансово-економічні показники підприємств-експортерів (у розрізі галузей промисловості), подано в спектральній карті, а кластер виділяє групи галузей, схожі за оцінкою рівня цих показників. Зазначимо, що темний колір клітинки означає інтенсивну вираженість характеристики, тоді як світлий – незначну. Чим сильніший контраст кольору клітинок, у яких містяться оцінки аналогічних показників, тим більш значуще відрізняються поміж собою галузі за тим, якою мірою їхні підприємства підвищують рівень фінансово-економічного показника.

До групи 1 ввійшли галузі – виробництво коксу, продуктів нафтопереробки і ядерного палива, а також виробництво інших неметалевих мінеральних виробів. Ці галузі найбільш схожі між собою за всіма фінансово-економічними показниками (найвищі показники), особливо за інвестиційною привабливістю та обсягами реалізації. До групи 2 ввійшли підприємства тих галузей промисловості (легка промисловість, лісова та переробна, целюлозно-паперова, виробництво меблів, агропромисловість, транспорт і зв'язок, електронна промисловість, устаткування для радіо, телебачення та зв'язку), що мають подібність між собою майже за всіма показниками (високі показники), але ж деякі фінансово-економічні показники набагато нижчі від аналогічних показників інших галузей.

В цілому отримані результати дозволять оцінити надійність різних методів прогнозування в сучасних «трансформаційних» умовах.

Науковий керівник — к.т.н. Василь Бриль

Система аналізу індексу цін на основі аналітичного апарату «Логос-Експерт»

УДК 004.658.6:330(477)(043.2)
Віктор Гловацький
Національний авіаційний університет, Україна, elkman@ukr.net

Ефективний соціально-економічний розвиток країни, державне управління та регулювання пов'язане з необхідністю своєчасного отримання та аналізу повної, достовірної, науково-обгрунтованої офіційної статистичної інформації про соціальні, економічні, демографічні, екологічні та інші суспільні явища.

Спостереження за зміною цін і тарифів на споживчому ринку ставить своїм завданням збір інформації про рівень цін і їх зміни на основі систематичної реєстрації на споживчому ринку.

Індекс цін - це показник, що характеризує зміну цін за певний період часу.

Метою роботи є аналіз, оцінка та прогнозування стану індексу цін протягом визначеного періоду. Модулем візуалізації для досягнення мети виступає пакет прикладних програм «Логос-Експерт» та вбудовані в нього математико-статистичні методи аналізу.

Своєчасний аналіз дає нам змогу швидко реагувати на зміни в економіці та прогнозувати майбутній плин речей. Це пояснює актуальність дослідження індексу цін. Дані індексу цін постійно оновлюються і змінюються, за рахунок цього виконана робота є потенційно новою і актуальною, так як викладений матеріал наданий в розрізі останніх років.

«Логос-Експерт» призначений для обробки даних та видобування «знань» в базах даних за допомогою математико-статистичних методів аналізу та еволюційних алгоритмів.

Аналіз та оцінка полягає в використанні таких методів аналізу як: 1) кореляція; 2) парна регресія; 3) частотний розподіл; 4) кластерно-спектральний аналіз; 5) багатовимірне шкалювання та ін.. В свою чергу прогнозування передбачає використання таких технологій, як нейронні мережі, дерево рішень та екстраполяція.

Вхідними даними є таблиці, а вихідними – сукупність графічної, текстової та числової інформації.

Темпи інфляції визначаються як величина зміни індексів цін, що, в свою чергу, є вираженням вартості набору товарів (послуг) в певний період часу. В сучасних умовах необхідно навчитися правильно та ефективно використовувати індекс цін в інтересах розвитку національної економіки. Комплексний аналіз забезпечує достовірною інформацією про поточний стан речей.

Отже, розроблений аналітичний звіт сприяє своєчасному та ефективному виявленню та аналізу негативних процесів в економіці з подальшим реагуванням та попередженням у майбутньому.

Науковий керівник — д.т.н. Володимир Бурячок

Аналітична система вибору засобу аналізу і оцінки ризиків

УДК 004.056.5(043.2)
Ганна Кудлюк
Національний авіаційний університет, Київ, kudlyuk-anna@mail.ru

Розвиток ІТ-інфраструктури підприємств призвів до зростання загроз і вразливостей інформаційної безпеки (ІБ). Загроза ІБ – сукупність умов і факторів, що створюють небезпеку життєво важливим інтересам особистості, суспільства і держави в інформаційній сфері. Потенційно ці умови і фактори можуть призвести до порушення основних властивостей інформації – доступності, цілісності і конфіденційності. Поняття «вразливостей інформаційної безпеки» розглядають як розширення можливостей доступу, що виникає в результаті помилок або особливостей проектування, програмування, експлуатації або стороннього втручання. Тісно пов'язана з поняттям «загроз» та «вразливостей» сутність ризику ІБ. Ризик ІБ– це імовірність того, що дана загроза буде експлуатувати вразливість активу і тим самим завдасть шкоду організації. Також ризик розглядають як фактор, що відображає можливий збиток організації в результаті реалізації загрози ІБ. В цих умовах оцінка інформаційних ризиків необхідна для визначення рівня захисту інформації, здійснення його підтримки і розробки стратегії розвитку інформаційної структури компанії. Оцінка та аналіз інформаційних ризиків є необхідною умовою при створенні системи менеджменту інформаційної безпеки, системи управління ризиками і плану забезпечення безперервності та відновлення бізнесу компанії.

В сучасному інформаційному просторі асортимент засобів оцінки ризиків ІБ досить різноманітний, а їх робота направлена на різні сфери діяльності підприємств та основана у відповідності до різних стандартів ІБ, тому визначення параметрів для класифікації та проведення систематизації вибору існуючих засобів оцінки ризиків ІБ є актуальним завданням. У зв'язку з цим метою роботи є визначення основних критеріїв та характеристик існуючих засобів оцінки ризиків ІБ для систематизації їх вибору.

В ході проведення аналізу засобів оцінки ризиків ІБ на основі їхніх характеристик та властивостей функціонування було визначено 15 найбільш розповсюджених. На основі аналізу досліджуваних засобів сформовано 9 основних параметрів (критеріїв) для систематизації їх вибору експертом: 1) Країна-розробник; 2) Сфера діяльності організацій; 3) Мова; 4) Масштаб організацій; 5) Стандарти; 6) Кількість етапів; 7) Компоненти для оцінки ризиків; 8) Міра ризику; 9) Вихідні дані. За допомогою C++Builder 2010 програмно реалізовано систему вибору засобів аналізу та оцінки ризиків. Створена система працює на основі сформованої в Database Tour 6 бази даних, відповідно із обраними експертом значеннями параметрів. Реалізована програмно система вибору засобів аналізу та оцінки ризиків, дозволяє експертам обирати продукти для оцінки ризиків ІБ на основі визначених параметрів. Система має практичне застосування в організаціях, які прагнуть покращити рівень ІБ системи чи розробити політику безпеки компанії.

Науковий керівник – к.т.н. Анна Корченко

Інформаційно-аналітична система синтезу механізмів захисту інформаційних ресурсів

УДК 004.056(043.2)
Олексій Лозовий
Національний авіаційний університет, Україна, cosmo83@yandex.ru

Для забезпечення захисту інформації в інформаційних системах на заданому рівні необхідно застосування механізмів захисту інформаційних ресурсів, що поєднуються в єдину систему захисту інформації. Теоретична база вивчення проблем, що виникають при проектуванні систем захисту інформації у даний час тільки формується, а процес аналізу і синтезу систем захисту інформаційних ресурсів дотепер не формалізований, що призводить до вартісних і часових витрат. Тому розробка інформаційно-аналітичної системи аналізу ефективності систем захисту інформаційних ресурсів і одержання практичних методів вибору механізмів захисту інформаційних ресурсів є актуальною проблемою, що має наукове і практичне значення.

Метою роботи є підвищення захищеності інформаційних ресурсів від кібератак за рахунок розробки інформаційно-аналітичної системи синтезу механізмів захисту.

Оцінка ефективності захисту виконується на рівні окремого механізму захисту, а її результати дозволяють визначити здатність відповідної системи захисту інформаційних ресурсів протистояти кібератакам. При виборі механізмів захисту повинні враховуватися можливості управління ними для забезпечення максимально можливого рівня захищеності. Застосування механізмів захисту інформаційних ресурсів впливає на імовірність реалізації кібератаки. Один з способів оцінки такого впливу заснований на заданні зниження коефіцієнтів небезпеки та імовірності реалізації загроз в умовах захисту інформації безпосередньо експертами за допомогою нечітких чисел.

Розроблено систему синтезу механізмів захисту інформаційних ресурсів, яка на основі методу впливу кібератак, моделі поводження атакованої інформаційної системи та вдосконаленої моделі системи захисту інформаційних ресурсів, дозволяє забезпечити заданий рівень захищеності.

Для перевірки роботи розробленої системи синтезу механізмів захисту інформаційних ресурсів розроблено програмний комплекс, що дозволяє змоделювати захист інформаційних ресурсів за обраними критеріями та рекомендує необхідні механізми захисту, які можуть протидіяти кібератаці. В якості об'єкта дослідження була прийнята складна система, призначена для збору, зберігання, обробки, передачі інформації, необхідної користувачеві.

При отриманні вхідних даних для проведення розрахунків використовуються інструментальні засоби, призначені для прийняття рішення, що базується на алгоритмах логічного виводу на основі системи правил, сформованих в умовах невизначеної інформації. Для завдання функцій належності та інтерпретації результатів використовувався пакет Fuzzy Logic Toolbox системи MATLAB. За рахунок використання ефективного набору механізмів захисту рівень захищеності інформаційних ресурсів збільшився на 2-11%. *Науковий керівник — к.т.н. Василь Бриль*

Аналітична система оцінки регіональних особливостей ринку банківського кредитування

УДК 336.77.067.21:657.422.1(043.2)
Анастасія Карбовнича
Національний авіаційний університет, Україна, n.d.karbovnichaya@gmail.com

На сьогодні найбільш динамічно розвиненим сегментом банківського ринку є кредитування. Кредитна діяльність банків є рушійним стимулом розвитку не лише банківської системи регіону, а й економіки в цілому. На кредитний ринок України значно вплинули негативні наслідки світової фінансово-економічної кризи, що вказало на високу вразливість його від зовнішніх чинників.

Банківські послуги активно впливають на розвиток економіки України і відіграють значну роль у задоволенні потреб населення, підвищенні його життєвого рівня шляхом надання споживчих кредитів і впливу на розвиток малого бізнесу. Це пояснює актуальність дослідження особливостей розвитку ринку банківського кредитування, зокрема створення аналітичної системи оцінки регіональних особливостей ринку банківського кредитування.

Метою розробки аналітичної системи є створення інструменту для аналізу, оцінки та прогнозування стану на ринку банківського кредитування у регіонах України протягом визначеного періоду, а також створення на основі отриманої інформації аналітичного звіту. Модулем візуалізації для досягнення мети є пакет прикладних програм «ЛОГОС» та вбудовані в нього математико-статистичні методи аналізу.

Новизною роботи є те, що вперше запропоновано аналітичну систему, що за рахунок використання різних методів оцінки і аналізу дозволяє на основі пакету прикладних програм «ЛОГОС» створити аналітичний звіт щодо стану різних галузей народного господарства (зокрема в галузі банківського кредитування).

Практична цінність полягає в тому, що розроблений аналітичний звіт сприяє своєчасному та ефективному втручанню у проблемні процеси банківського кредитування, де необхідне підвищення ефективності діяльності, та впливає на процес прийняття управлінських рішень.

Аналіз та оцінка полягає в використанні таких методів аналізу: 1) основні статистики; 2) групові середні; 3) частотний розподіл; 4) кластерно-спектральний аналіз; 5) багатовимірне шкалювання; 6) позиційний радар; 7) класифікація; 8) поверхня. У свою чергу, прогнозування передбачає використання таких технологій, як нейронні мережі, дерево рішень та екстраполяція. Для кожного з методів вхідними даними є таблиці, а вихідними – сукупність графічної, текстової та числової інформації.

Таким чином, завдяки використанню різних методів аналізу можна дослідити та оцінити реальну ситуацію на ринку та її основні недоліки, а завдяки прогнозуванню – передбачити розвиток певного сегменту ринку та його взаємодію з іншими сегментами в найближчий час. На основі отриманих даних створений аналітичний звіт, що містить висновки, основні поради та пропозиції. *Науковий керівник — к.т.н. Сергій Гнатюк*

Система індикаторів рівня розвитку інформаційно-комунікаційних технологій в Україні

УДК 004.4(043.2)
Кульчицький Олександр
Національний авіаційний університет, Україна, kulchizki@yandex.ua

Система індикаторів розвитку інформаційно-комунікаційних технологій (ІКТ) являє собою комбінований показник, що характеризує досягнення країн світу з точки зору розвитку інфокомунікаційної сфери.

Одним з головним пріоритетів при розбудові економіки знань в Україні є подальший розвиток інформаційного суспільства, що передбачає: прискорення розробки та впровадження інформаційно-комунікаційних технологій в усі сфери суспільного життя; необхідність збільшення різноманітності та кількості послуг населенню й бізнесу на основі ІКТ; створення загальнодоступних електронних інформаційних ресурсів тощо. Саме останнє суттєво загострює проблему якісного розвитку та створення адекватного механізму оцінювання й аналізу ІКТ як в цілому по Україні, так і в її регіонах.

В Україні дане питання досліджували Д. В. Дубов, О. Є. Бавико, О. Б. Баховець, С. К. Полумієнко, Л. О. Рибаков, В. В. Тюрін, які розглядали системи індикаторів ІКТ в суспільстві та економіці. На державному рівні формуванням системи індикаторів ІКТ покладене на Державне агентство з питань науки, інновацій та інформатизації.

В даний час існує кілька міжнародних рейтингів, які прямо чи опосередковано характеризують рівні розвитку ІКТ та зрілості інформаційного суспільства в різних країнах світу, а саме: 1) рейтинг Організації об'єднаних націй (рейтинг розвитку електронного уряду - E-government development rank). Включає оцінки таких аспектів як електронні послуги, що надаються органами влади, інформаційно-комунікаційна інфраструктура та розвиток людського потенціалу; 2) рейтинг Міжнародного союзу електрозв'язку (індекс розвитку ІКТ - ICT Development Index), який визначає світові стандарти в області ІКТ. Ці показники стосуються доступу до ІКТ, використання ІКТ, а також навичок, тобто практичного знання цих технологій населенням країн, охоплених дослідженням; 3) рейтинг Всесвітнього економічного форуму (індекс економіки знань - Knowledge Economy Index). Характеризує загальний рівень продвинення країни чи регіону до економіки, основаної на знаннях); 4) рейтинг Всесвітнього банку (Рейтинг кіберпотужності - Cyber Power Index). Відображає здатність країн протистояти кібератакам і розгортати критичну цифрову інфраструктуру, необхідну для формування продуктивної і безпечної економіки.

Розглядаючи існуючі міжнародні рейтинги, що характеризують рівні розвитку ІКТ, бачимо, що вони є доволі всеохоплюючими. Тому при впровадженні та розвитку інформаційно-комунікаційних технологій на теренах нашої держави вони потребують певної деталізації у вивченні, а також відповідного узагальнення та корегування.

Науковий керівник — д.т.н. Володимир Бурячок

Параметры прогнозирования и идентификации атак в информационно-коммуникационных системах

УДК 004.056.53:004.492.3
Андрей Гизун, Станислав Топчеев
Національний авіаційний університет, Украина, TopcheevS.KJ@bigmir.net, andriy.gizun@gmail.com

Концепция управления непрерывностью бизнеса (УНБ) предусматривает ряд этапов, наиболее важными среди которых есть анализ влияния на бизнес, прогнозирование и идентификация кризисных ситуаций (КС), реагирование на КС, устранение их последствий и восстановление бизнес-процессов, прерванных КС, а также документальное обеспечение систем УНБ. Любая кризисная ситуация является последствием совокупности инцидентов или атак. Исходя из этого определения и формализации основных параметров, которые могут быть использованы для выявления и идентификации компьютерных атак, безусловно, являются актуальной задачей. Для эффективного предупреждения КС в сфере ИБ необходимо разработать набор ключевых параметров для прогнозирования и идентификации атак на ИКС, которые при определенных условиях могут быть причинами возникновения кризиса. Таким образом, целью данной работы есть определение (формализация) основных параметров, значение и характер изменения которых могут определить возможность реализации той или иной атаки.

Чтобы спрогнозировать возможность реализации атаки или выявить ее и идентифицировать необходимо разработать систему, которая будет производить мониторинг сетевых характеристик и локальных (хостовых) характеристик. Учитывая то, что реализация КС может иметь как предопределенный так и случайный характер, а ИКС есть по своей сути слабоформализованной средой, то система должна быть основана на специальных методах теории нечетких множеств , а следовательно некоторые из используемых параметров могут быть нечеткими по своей природе. Рассмотрим и проанализируем параметры, контролируемые системой для прогнозирования, выявления и идентификации атак в ИКС:

Загрузка ЦП, CPU – процентный показатель процессорного времени, выделенного на выполнение задач. По уровню загруженности можно определить насколько сильно компьютер подвержен вредоносным воздействиям. Параметр является нечетким, так как ее оптимальное (нормальное) значение различно для разных систем и, к тому же, не дает четкого ответа о наличии факта атаки..

Загруженность сетевого канала, CNCh. Мониторинг трафика позволяет фиксировать данные, которые передаются по интернет-каналу. Значительное возрастание трафика свидетельствует о возможной DDos-атаке или другой атаки. А поскольку величину нормальной загруженности сетевого канала определить практически невозможно, то параметр есть нечетким.

Несвойственные процессы, UPr. Наблюдая за количеством процессов, можно определить какой процесс есть новым и может быть вредоносным. Параметр является точным, так как количество процессов ограничено, в

начале работы система мониторинга делает так называемый снимок системы и новые процессы всегда можно просмотреть и перечислить.

Размер временных файлов, STF. Во временных файлах может храниться копия вируса, либо резервное тело вируса для автоматического запуска. Параметр является нечетким из-за того что слишком много разных временных файлов создаётся и удаляется во время работы компьютера и размер их при нормальном функционировании может быть различным.

Открытие неиспользуемых портов, OUP. Параметр является четким, вначале работы системы мониторинга делается снимок системы (открытые порты), а появление в процессе работы новых открытых портов может служить сигналом о атаке на ИКС.

Загруженность оперативной памяти, MU. Нечеткий параметр, по своей природе аналогичен с параметром загрузка ЦП.

Количество сбоев и ошибок, NEr. В эту группу входит широкий спектр событий от ошибок при авторизации к сбоям при выполнении определенных процессов или файлов. Так большая интенсивность возникновения ошибок и сбоев свидетельствует с некоторой вероятностью о возможности реализации атак. Этот параметр относится к нечетким, так как ошибки очень часто являются элементом нормальной работы системы в ИКС из-за технических характеристик аппаратного и программного обеспечения..

Изменений структуры и размера файлов, ChSSF. Этот параметр есть четким при условии, что процессы работы легальных пользователей постоянно контролируются и регламентированы правилами политики безопасности в ИКС. Количество одновременных подключений, NCC. Как показывает практика для эффективного проведения DDoS необходимо привлечение большого количества источников, участвующих в нападении на жертву. Следовательно, параметр NCC при увеличении количества подключений к серверу может использоваться в качестве одного из признаков начала атаки. Параметр является нечетким, так как при небольших значениях характерен и для состояния нормального функционирования и точное значение, которое может свидетельствовать об атаке, определить практически невозможно.

Задержка между запросами от одного источника, DbR. Параметр характеризует время между последовательными запросами от одного подключенного к серверу клиента. Уменьшение задержки между запросами может свидетельствовать о начале DDoS-атаки. Этот параметр также есть нечетким.

Рассмотренные в работе параметры создают кортеж выявления и идентификации атак:

DIA = <CPU, CNCh, UPr, STF, OUP, MU, NEr, ChSSF, NCC, DbR>.

Выводы. Таким образом, в этом исследовании определено значение параметров кортежа выявления и идентификации атак, которые должны контролироваться системой для прогнозирования атак на ИКС. Формализация этих параметров разрешает учитывать особенности атак в ИКС и увеличить эффективность превентивных средств и систем защиты информационных ресурсов.

Захист інформаційних ресурсів за допомогою файлової системи StegFS

УДК 004.056(043.2)

Віктор Самусь, Роман Макарчук
Національний авіаційний університет, Україна, textnice@gmail.com, verten2010@meta.ua

Для впорядкування даних на жорстких дисках використовується певна базова структура, яка називається файловою системою. Основним недоліком сучасних файлових систем (зокрема NTFS, FAT32, FAT та HFS+) є значний їх вплив на продуктивність і використання дискового простору (особливо це актуально для дисків великої місткості) у процесі захисту інформації від несанкціонованих користувачів. Одним із варіантів вирішення цієї проблеми, як і низки інших, є використання стеганографічної файлової системи StegFS, яка працює на базі операційної системи Linux. Проте, система StegFS не є повністю дослідженою, що ускладнює усвідомлення її переваг з боку пересічних користувачів. З огляду на це, метою роботи є дослідження можливостей StegFS як засобу забезпечення ефективної безпеки інформаційних ресурсів.

Як показав аналіз, система StegFS фактично приховує дані на жорсткому диску, роблячи їх візуально відсутніми для користувачів. Ця технологія є ефективною для розв'язання задач захисту інформації (зокрема забезпечення конфіденційності інформаційних ресурсів), оскільки забезпечує не лише шифрування (криптографічних захист), а й приховування її наявності (стеганографічний захист). Система має можливість використання довільно згенерованих шаблонів. Крім того, StegFS додатково підтримує один або більше помилкових прихованих файлів, які вона періодично оновлює. Це необхідно для того, щоб утримати зловмисника від припущення, що блоки, які розміщені в бітовому масиві і не належать жодному простому файлу, можуть містити приховані дані. Число (кількість) таких файлів може налаштовуватись вручну або автоматично. Оскільки приховані файли не заносяться в центральну директорію, StegFS повинна мати можливість пошуку заголовку файлу, використовуючи тільки ім'я файлу і ключ. Під час створення файлу StegFS використовує хеш- значення, обчислене з імені файлу і ключа для генератора випадкових номерів блоків. Потім, кожен успішно згенерований блок, система переглядає у бітовому масиві доти, поки не знайде вільний блок для збереження у ньому заголовку. Після того як заголовок збережений, наступні блоки можуть бути призначені довільно, узгоджені з бітовим масивом, а потім приєднані до індексного дескриптора таблиці файлу.

Таким чином, використання файлової системи StegFS є одним із ефективних сучасних методів забезпечення безпеки інформаційних ресурсів. Використання StegFS дозволяє користувачам операційної системи Linux обмінюватись прихованими файлами і обмежувати доступ до цих файлів нелегітимним користувачам.

Науковий керівник — к.т.н. Сергій Гнатюк

Захищений мережевий клієнт для IP-телефонії

УДК 004.056.5:621.395
Євгеній Бондарь, Ірина Лозова
Національний авіаційний університет, Україна, eugene.bond277@gmail.com, kira1983@yandex.ru

Все більшої популярності серед бізнес-користувачів в усьому світі набувають телекомунікаційні рішення на основі технологій VoIP. Український комерційний сектор користувачів активно переходить з традиційної PSTN телефонії на технології VoIP. Натомість, рішення для малого та середнього бізнесу, а також для звичайного користувача залишаються вразливими для найпростіших атак. Метою роботи є організація захищеного телефонного зв'язку за допомогою софтфону між клієнтом та сервером, використовуючи методи автентифікації та авторизації, а також мережеві протоколи, які забезпечують шифрування, встановлення автентичності повідомлення, цілісності, захист від заміни даних. Для реалізації механізмів захисту VoIP технологій використовуємо відкриті протоколи засновані на стандартах RFC, оскільки це надає можливість взаємодіяти з програмним та апаратним забезпеченням сторонніх виробників. Захист IP-телефонії можна умовно поділити так: захист на рівні встановлення з'єднання, захист на рівні передачі медіа даних. Зокрема, дані протоколу SIP, захищаємо за допомогою протоколів транспортного рівня – TLS. Використання протоколів TLS забезпечить конфіденційність адресата, та унеможливить перенаправлення дзвінку. Передачу медіа даних захищаємо шляхом використання протоколів SRTP, SRTCP та ZRTP. Протокол ZRTP забезпечить узгодження ключів шифрування, SRTCP використовується для контролю медіа сесії, а SRTP відповідає за аутентифікацію, шифрування та пересилання медіа даних. Загальну схему можна зобразити так:

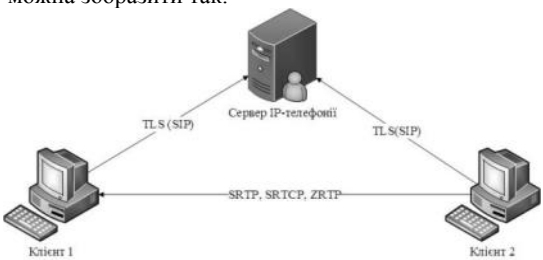

Рис. 1 Схема організації захищеного телефонного зв'язку

Для організації захищеного з'єднання можна використовувати технології VPN, IPsec або деякі закриті технології та протоколи відомих брендів. Якщо ж використовувати софтфон із підтримкою безпечних мережевих протоколів, ми отримуємо захищене з'єднання, без витрат на дороге брендове обладнання, надзвичайно мобільну організацію зв'язку, можливість інтеграції з іншими мережевими та системними сервісами (взаємодія з базами даних, можливість здійснення конференц-зв'язку, взаємодія з іншим офісним ПЗ).

Науковий керівник — к.т.н. Євгенія Іванченко

Деякі аспекти захисту громадянського суспільства від інформаційної зброї

УДК 32:004

Богдан Кобільник, Владислав Гріга
Національний авіаційний університет, Україна, gsm-grey@mail.ru, gsm-grey@rambler.ru

Сучасний інформаційний простір набув дуже важливого значення у розвитку цивілізації. З його популяризацією та розширенням виникають певні проблеми, які становлять досить серйозну загрозу. За допомогою інформації можна контролювати думки великої кількості людей – цю властивість почали активно використовувати у теперішній політиці, міждержавних конфліктах і різного роду протистояннях (інформаційному протиборстві). В Україні сьогодні проходить глобальний процес інформатизації суспільства, він займає важливе місце у розвитку держави в цілому і водночас містить певні специфічні загрози. З огляду на це, актуальним є дослідження нових загроз, які виникли у процесі інформатизації суспільства. Метою дослідження є аналіз захищеності інформаційного простору нашої держави, виявлення його уразливостей та формулювання пропозицій щодо їх усунення.

Дослідження починаємо із аналізу нещодавніх подій у світі. Конфлікт у Південній Осетії 2008 року став яскравим прикладом інформаційної війни – події висвітлювались у настільки неправдивих значеннях, що світова спільнота не могла побачити реальні факти. Крім того, нещодавно ми стали очевидцями інформаційної експансії із сторони східних сусідів на український інформаційний простір, яка триває і дотепер. Основна атака йшла через інформаційно-телекомунікаційні системи у вигляді потоку недостовірної і провокуючої інформації, що, у певні мірі, сприяло від'єднанню АР Крим від України. Процес захисту інформаційного середовища, що задекларований у нормативно-правових актах, є недосконалим. Проводячи аналіз основних таких актів, стає помітним, що наша інформаційна оборона є недостатньо матеріально забезпеченою і відсутній орган, який має займатись саме такими питаннями. Досвід розвинених держав (зокрема Японії, США і ЄС) вказує на необхідність створення спеціальних частин війська (кіберпідрозділів), які мають відповідати за інформаційну (кібернетичну) безпеку держави. Як показали останні політичні події, Україні вкрай необхідні схожі формування у складі ЗСУ для захисту інформаційного простору від зовнішніх інформаційних та кібернетичних впливів. Крім того, потребують модернізації спеціалізовані департаменти СБ та СЗР України, відповідальні за захист інтересів держави в інформаційній сфері. Також, необхідно активно залучати ЗМІ для висвітлення громадськості тільки достовірної інформації і зменшення впливу ворожих телемедіа. Такі заходи будуть корисними, ефективними і не збитковими з огляду на втрату частини держави і загрози суверенітету України.

Таким чином, проведений аналіз вказує на недостатню захищеність громадянського суспільства від впливу інформаційної зброї. У роботі, на основі міжнародного досвіду, визначено пріоритетні шляхи захисту інформаційного простору України в умовах інформаційного протиборства.

Науковий керівник — к.т.н. Сергій Гнатюк

Комплексна система захисту інформації автоматизованої системи класу 3 юридичної фірми

УДК 004.056:004.75(043.2)
Білий Євгеній
Національний авіаційний університет, Україна, jeh9beliy@gmail.com

Витік будь-якої інформації може відобразитися на діяльності організації. Особливу роль відіграє конфіденційна інформація, втрата якої, зазвичай, призводить до значних матеріальних збитків. Повноцінний захист конфіденційної інформації забезпечується проведенням комплексного аналізу каналів витоку і методів несанкціонованого доступу до інформації. Тому розробка та впровадження комплексної системи захисту інформації (КСЗІ) підприємства в даний час дуже актуальні і важливі.

Метою роботи є створення КСЗІ автоматизованої системи (АС) класу 3 юридичної фірми, що включає в себе: формування моделі загроз інформації та моделі порушника об'єкта інформаційної діяльності, розробку політики безпеки та системи документів із забезпечення захисту інформації в АС, а також розрахунок та оцінку ризиків.

Процес створення КСЗІ полягає у здійсненні комплексу взаємоузгоджених заходів, спрямованих на розроблення і впровадження інформаційної технології, яка забезпечує обробку інформації в АС згідно з вимогами, встановленими нормативно-правовими актами та нормативними документами у сфері захисту інформації. КСЗІ створюється на основі Закону України «Про захист інформації в інформаційно-телекомунікаційних системах», ДСТУ 3396.1-96, НД ТЗІ 1.1-002-99, НД ТЗІ 1.4-001-2000, НД ТЗІ 2.1-001-200, НД ТЗІ 3.7-001-99, НД ТЗІ 3.7-003-05.

Розробка та впровадження КСЗІ дозволить: 1) керувати доступом до ресурсів АС для захисту від випадкового або навмисного втручання в роботу системи та несанкціонованого доступу до інформації; 2) забезпечити захист інформації, що передається по каналам зв'язку; 3) забезпечити реєстрацію, збір, збереження, обробку та видачу відомостей про всі події, що відбуваються в АС та мають відношення до її безпеки; 4) забезпечити контроль роботи користувачів системи зі сторони адміністрації; 5) забезпечити контроль і підтримку цілісності критичних ресурсів системи; 6) забезпечити управління засобами системи захисту.

В роботі було проведено аналіз існуючих підходів до побудови КСЗІ підприємства. Розроблено технічне завдання, що містить в собі основні вимоги до системи захисту. Укладено нормативну документацію підприємства з дотриманням вимог законодавства України та національних стандартів, узявши за основу перелік документів, які наведені у методичних рекомендаціях. Розроблено КСЗІ АС класу 3 для юридичної фірми відповідно до НД ТЗІ та вимог технічного завдання. Проведено тестування та атестацію керівництвом організації, а також підготовку до проведення державної експертизи.

Науковий керівник — Ірина Лозова

Актуальність створення центрів реагування на інциденти для приватної сфери

УДК 004.056.5(043.2)
Юлія Бугай
Національний авіаційний університет, Україна, ms.Ater@mail.ru

В усі часи питання захисту інформаційних ресурсів від сторонніх осіб було дуже важливим. Із розвитком техніки та глобальною інформатизацією суспільства все більша увага почала приділятися різним методам секретного обміну інформацією. З появою нових засобів передачі та обробки даних, зокрема Інтернету, суспільство отримало канал зв'язку, що одночасно є і достатньо швидкісним, і ненадійним з точки зору інформаційної безпеки. Саме тому, є актуальною робота центрів (груп) реагування на інциденти типу CERT/CSIRT (далі – CERT). Більшість таких центрів (наприклад, CERT-UA) орієнтовані на захист державних інформаційних ресурсів, приватні ж організації змушені боротися з кібератаками своїми силами, а отже, потребують допомоги кваліфікованих фахівців. Інформацію щодо діяльності CERT/CSIRT можна знайти на сайтах окремих центрів, а також міжнародних організацій ENISA та FIRST. Крім того, у фахових наукових журналах «Безпека інформації» та «Захист інформації» було опубліковано низку робіт присвячених діяльності зазначених структур та системам управління інцидентами інформаційної безпеки (ІІБ). Метою дослідження є доведення необхідності створення в Україні групи реагування на ІІБ, яка б займалася захистом інформаційних ресурсів у приватній сфері і, таким чином, централізувала би боротьбу з ІІБ, не пов'язаними з державним сектором. Як показує міжнародна практика, окремі зусилля дають набагато гірший результат, ніж спільні. Саме тому, усі світові центри CERT об'єднані в одну глобальну мережу з метою обміну інформацією про ІІБ та способи їх якнайшвидшого усунення. Сьогодні в Україні функціонує лише одна організація такого типу – CERT-UA, але вона займається захистом виключно державних інформаційних ресурсів. Група CERT-UA керується такими нормативними актами, як Закон України «Про Державну службу спеціального зв'язку та захисту інформації України», Закон України «Про телекомунікації», деякими постановами КМУ та наказами Держспецзв'язку. Приватні організації процес управління ІІБ покладають на службу ІТ-підтримки, яка через це змушена відволікатися від своїх основних обов'язків. Крім того, деякі міжнародні механізми захисту можуть бути не адекватними існуючій у державі ситуації чи не мати необхідного сертифіката державного зразка. Отже, маємо істотну проблему, яку можна вирішити лише за допомогою створення централізованого органу, що займався б її вирішенням виключно у приватному секторі. Якщо ж такий орган співпрацюватиме із CERT-UA, то він зможе, на основі розширеної бази даних та досвіду, ефективно реагувати на ІІБ за рахунок зростання швидкості та коректності прийняття рішень.

Таким чином, створення групи CERT/CSIRT для приватної сфери України є необхідним кроком для підвищення ефективності реагування на ІІБ та загального рівня інформаційної безпеки держави.

Науковий керівник – аспірант Віктор Гнатюк

Програмний модуль визначення коефіцієнтів важливості для експертиз інформаційної безпеки

УДК 65.012.8(043.2)
Наталія Вишневська, Олександр Боднарчук
Національний авіаційний університет, Україна, a_ndrey93@mail.ru

Прийняття управлінських рішень є відповідальним процесом у будь-якій сфері діяльності людства, в тому числі і в галузі інформаційної безпеки. Для підвищення ступеня об'єктивності та якості процедури прийняття рішень доцільно враховувати думки не лише одної особи, що приймає рішення, а декількох. З цією метою проводиться групова експертиза. Для узагальнення результатів експертизи доцільно використовувати коефіцієнт важливості (КВ), який відображає переваги експерта. Тому створення програмного засобу визначення коефіцієнтів важливості для використання експертами під час вирішення багатокретиріальних задач є актуальною задачею. Метою роботи є розробка програмного модуля визначення коефіцієнтів важливості на основі різних груп методів. Новизною роботи є те, що розроблено програмний засіб визначення коефіцієнтів важливості кількісними та якісними методами відповідно до інформації, яка надходить від експертів.

Групова експертиза включає в себе два етапи: формування експертної комісії та експертне оцінювання. Типова схема формування експертної комісії включає такі етапи, як визначення кількісного складу експертної комісії, розробка формальних і професійних вимог до експерта, оцінка ступеня компетентності кожного експерта. Правильний відбір фахівців для участі в роботі експертної групи дуже важливий, тому що якість отриманих оцінок в значній мірі визначається якістю експертної групи. Якість і кількість експертів враховуються при формуванні експертної групи та обробці результатів експертного опитування. Експертне оцінювання проводиться сформованою експертною групою. В ході експертизи формуються різноманітні параметри, які треба коректно обробити та узагальнити для отримання кінцевих результатів експертизи. Початковою інформацією для обробки є судження, що відображають переваги експертів, у числовій і лінгвістичній формі, тому є необхідність використання якісних і кількісних методів обробки результатів.

У зв’язку з цим в розробленому модулі для визначення КВ пропонується застосовувати як якісні, так і кількісні методи, відповідно до інформації, яка надходить від експертів. Якісні методи придатні для тих випадків, коли метою експертизи є отримання якісних оцінок певних критеріїв об’єкту, визначення найкращої альтернативи, а кількісна характеристика носить другорядний характер. В іншому випадку, коли необхідно отримати числові оцінки, використовують кількісні методи. Вибір методу визначення КВ здійснюється безпосередньо експертом під час проведення експертизи в залежності від мети експертизи. Розроблений програмний засіб може використовуватись для визначення коефіцієнтів важливості під час проведення експертизи, в тому числі для експертиз інформаційної безпеки.

Науковий керівник — Юлія Бойко

Програмний модуль оцінки захищеності підприємства від соціотехнічних атак

УДК 65.012.8(043.2)
Ольга Котік, Дмитро Вобліков
Національний авіаційний університет, Україна, voblikovd@gmail.com

Соцотехнічні атаки на сьогоднішній день являють серйозну загрозу безпеці будь-якого підприємства, в тому числі державної установи. Тому потрібно своєчасно виявляти слабкі ланки для запобігання серйозним витокам інформації, використовуючи сучасні методи та засоби виявленВиходячи Виходячи з вищесказаного розробка програмного модуля оцінки захищеності підприємства від соціотехнічних атак є актуальною.

Метою роботи є розробка програмного модуля для виявлення слабких до соціотехнічних атак місць з метою підвищення рівня безпеки підприємства. Новизною роботи є те, що програмний модуль розроблений на основі проблемно-орієнтованих тестів та створених реєстраційних баз даних, він дозволяє оцінити захищеність підприємств від соціотехнічних атак, та прослідити динаміку їх зміни.

В процесі роботи з метою розробки способів протидії були досліджені соціотехнічні атаки, методи і засоби їх реалізації та визначено їх характерні ознаки. На основі отриманих даних був сформований загальний алгоритм здійснення будь-якої соціотехнічної атаки. Даний алгоритм був покладений за основу при розробці модуля.

Була зібрана статистика вторгнень за останні п’ять років, яка показала співвідношення випадкових та навмисних витоків даних. Співвідношення навмисних і випадкових витоків для всіх типів організацій мало відрізняється від глобального показника, з чого можна зробити висновок, що відсоток концентрації зловмисників і неакуратних співробітників не залежить від типу організації. Фактори, що призводять до випадкових витоків, діють однаково для менеджерів, чиновників і звичайних співробітників. Оскільки проблема внутрішніх загроз нині є дуже актуальною для будь-якого підприємства було вирішено створити програмний модуль, який дає можливість оцінити захищеність підприємства за допомогою виявлення соціотехнічних атак.

Розроблений програмний модуль являє собою психологічний тест, який направлено на виявлення у співробітників рівня уважності, потенційно небезпечних намірів, недобросовісності. Програма дуже проста в використанні, і може використовуватись будь-яким підприємством, в тому числі і державним, з врахуванням специфіки роботи. Особливо корисною дана програма буде в відділах кадрів при прийомі нових співробітників на роботу, а також для періодичного оцінювання інших співробітників. Але жодне програмне забезпечення без людського фактора не буде дієвим на 100%, тому для більш точних результатів необхідно біде провести ще бесіду з персоналом для біль точного результату тестування.

Науковий керівник — Юлія Бойко

Сучасні генератори псевдовипадкових послідовностей та рекомендації щодо їх застосування

УДК 004.421:519.246(043.2)
Надія Дуксенко, Тарас Паращук
Національний авіаційний університет, Україна, nadya-duks@yandex.ru, taras1039@gmail.com

На даному етапі розвитку інформаційних технологій, коли вони масово впроваджуваються в усі сфери людської діяльності, інформація з обмеженим доступом потребує ретельного захисту. Його можна забезпечити використовуючи криптографічні системи захисту інформації. Сьогодні криптографія має низку проблем, основною з яких є ефективне генерування ключових даних. Генератор псевдовипадкових послідовностей (ГПВП) – апаратний засіб (може також бути програмним чи програмно-апаратним), який використовує алгоритм, що генерує послідовність чисел, елементи якої майже незалежні один від одного і підвласні заданому розподілу. Він повинен відповідати таким вимогам: бути криптографічно стійким, мати позитивні статистичні властивості та великий період формованої послідовності, ефективно реалізовуватись апаратно і програмно.

Метою цієї роботи є аналіз сучасних ГПВП, оцінка їх переваг і недоліків та формування рекомендацій для покращення криптографічних властивостей.

У сучасних умовах для отримання випадкових послідовностей застосовують різноманітні ГПВП, які поділяються на дві групи – апаратні та програмні. Перша базується на використанні деяких фізичних явищ (шум в електронних приладах, різні фізичні шуми), тому їх використання вимагає наявності спеціального обладнання. У зв'язку з цим, більш зручним вважається застосування програмного ГПВП. Він являє собою програму, яка генерує послідовність чисел за певним алгоритмом. Така послідовність цілком детермінована (визначена), тобто принципово не може бути випадковою, її називають гаммою шифру. Період гамми – це та кількість псевдовипадкових чисел (ПВЧ) у послідовності, після якої вони починають повторюватись.

У ході роботи були розглянуті різні криптостійкі методи формування псевдовипадкових послідовностей (ПВП) на основі блокових та потокових шифрів. До криптостійких ГПВП відносяться генератори, побудовані на основі потокових шифрів, наприклад, генератори SEAL, RC4, RC5, RC6, Grain та інші. Основною їх перевагою є висока швидкість перетворення порівняно зі швидкістю надходження вхідної інформації, що забезпечує формування ПВЧ у реальному масштабі часу. До недоліків можна віднести необхідність синхронізації на приймальній та передаючій сторонах. Іншим класом криптостійких генераторів є ГПВП, побудовані на блокових шифрах. Їх робота полягає в застосуванні до блоку відкритого тексту багаторазового математичного перетворення. Основною перевагою є хороші статистичні властивості формованої ПВП і стійкість до різних видів криптоаналізу (кореляційний, інверсний та ін.). Їх недоліками є нечутливість криптосхем до випадання або вставки цілого числа блоків, існування проблеми останнього блоку неповної довжини тощо.

Атаки на ГПВП спрямовані на розкриття його параметрів з метою подальшого передбачення ПВП. Здатність ГПВП протистояти атакам зловмисників називається стійкістю. Атаки на ГПВП можна поділити на класи, які, в свою чергу, поділяються на такі види: 1) прямі криптоаналітичні атаки (за частковим попереднім обчисленням та за часом); 2) атаки на основі вхідних даних (з відомими вхідними даними, з відтворюваними вхідними даними, з вибраними вхідними даними); 3) атаки на основі розкриття внутрішнього стану (атаки постійного компромісу та повернення, атака «зустріч посередині», атака ітераційного вгадування); 4) кореляційні атаки (атака Зігентейлера, швидка кореляційна, атака на основі використання конволюційних кодів та відновлення лінійних поліномів); 5) спеціальні атаки (аналітичні, алгебраїчні, статистичні).

Одним з кращих ГПВП є генератор ANSI X9.17. Його схема складається з 112 – бітових ключів (K1, K2) і трьох EDE-шифрувань («зашифрування-розшифрування-зашифрування» з використанням алгоритму потрійного DES з двома ключами). На вхід подається два ПВЧ: значення дати і часу – DTi та початкове значення чергової ітерації. На виході формується початкове для наступної ітерації та чергове ПВЧ Ri. Якщо навіть Ri буде скомпрометовано, розрахувати Vi+1 та наступне ПВЧ Ri+1 з Ri неможливо, оскільки для отримання Vi+1 додатково виконується три операції EDE. Тоді:

Ri = EDEK1, K2 [EDEK1, K2 [DTi] Vi] Vi+1 = EDEK1, K2 [EDEK1,K2[DTi] Ri]

Стійкість генератора ANSI X9.17 досягається такими процедурами: використовується ключ – 112 бітів; введення дати і часу у вигляді 64-х бітів забезпечує якісну мітку часу, що запобігає атаці відтворення. Його недоліком є висока складність перетворень, так як не достатнім є період повторення.

На основі аналізу переваг і недоліків сучасних ГПВП можна сформувати такі рекомендації щодо їх ефективного застосування: 1) використовувати алгоритм генераторів з непостійним періодом, але достатнім для необхідної ПВП; 2) для підвищення надійності та стійкості доцільно використовувати не програмні, а програмно-апаратні генератори, швидкодія яких несуттєво відстає від програмних; 3) простота реалізації генератора, що полягає у можливості його запускання на примітивному апаратному забезпеченні; 4) працездатність генератора у режимі реального часу (введення параметрів самим користувачем або вони вибираються з сигналу звукової, відеокарти комп'ютера або інших системних параметрів); 5) генерування кожного біта ПВП з новим початковим станом, що у багато разів ускладнює реалізацію «брутального зламу»; 6) неможливість передбачення послідовності, знаючи попереднє значення.

Отже, в ході роботи було проаналізовано ГПВП різних типів. Дослідження показали що не існує ідеальної моделі генератора, вони повинні задовольняти вимоги різних оціночних тестів та проходити низку експертиз перед своїм використанням у криптосистемах. Вихідні дані ГПВП сьогодні використовуються в багатьох криптографічних системах для генерації ключів

та загальносистемних параметрів. Проведений аналіз можливих криптоатак та інших характеристик ГПВП визначив подальші напрямки розробки та реалізації ефективних і надійних генераторів.

Науковий керівник — к.т.н. Сергій Гнатюк

Програмний модуль захисту даних для телекомунікаційних каналів загального користування

УДК 004.056.55(043.2)
Юлія Бойко, Андрій Козлов
Національний авіаційний університет, Україна, a_ndrey93@mail.ru

З поширенням електроного документообігу все більше користувачів обмінюються інформацією з використанням відкритих телекомунікаційних каналів загального користування. Під час такого обміну передаються дані різного ступеня важливості, починаючи від простих текстових повідомлень і закінчуючи особистими даними та інформацією для службового користування. У зв'язку з цим актуальним питанням є розробка засобу захисту з урахуванням ступеня важливості передаваємих даних.

У зв'язку з цим метою роботи є розробка програмного криптомодуля на основі сучасного критпографічного алгоритму з можливістю його адаптації для захисту даних в залежності від ступеня їх важливості. Новизною роботи є те, що розроблени програмний криптомодуль забезпечує надійний захист даних, за рахунок використання стійкого крипто алгоритму, а можливість зміни довжини ключа безпосередньо користувачем робить модуль легкоадаптованим для потреб забезпечення захисту даних в залежності від ступеня важливості.

Аналіз ринку програмних засобів криптографічного захисту інформації показав, що останнім часом збільшується їх роль оскільки вони просто і доступно побудовані та не потребують великих фінансових витрат, в порівнянні з апаратними. Ці обставини призводять до того, що на ринку з'являється безліч засобів криптографічного захисту інформації, про які ніхто не може сказати нічого певного. При цьому розробники тримають криптоалгоритм (як показує практика, часто нестійкий) в секреті. Тому в основі розробленого програмного модуля було вирішено покласти безумовно стійкий криптографічний алгоритм.

В роботі було розроблено програмний модуль захисту даних, який засновано на криптографічному алгоритмі Blowfish. Даний алгоритм є досить надійним, а те, що він не є запатентований дозволяє його вільно використовувати для побудови власних систем захисту даних. Перевагою використання даного крипто алгоритму є те, що в ньому є можливість підтримки змінної довжини ключа від 128 до 448 біт.

Можливість зміни довжини ключа робить даний програмний модуль легкоадаптованим для потреб забезпечення захисту даних з різним ступенем важливості. Зашифрована інформація за допомогою даного модуля може передаватись відкритими телекомунікаційними каналами, а її власник може бути певним в збереженні її конфіденційності.

Системи захисту та обміну даними в складних технічних системах

УДК 004.056
Володимир Любченко
Національний авіаційний університет, Україна, vov_l@mail.ru

Надійність і стабільність роботи крупних розподілених систем в сучасних умов залежить від застосування засобів автоматизації і належності технологічних обробляючих систем управління. Саме системи автоматики, збору інформації, автоматизації керування на всіх рівнях забезпечують надійність виробництва.

Якщо раніше проблема захисту інформації була надбанням тільки спеціальних служб, то згодом вона стала актуальною для всіх організацій та підприємств, а особливо для підприємств авіаційної промисловості України, так чи інакше пов'язаних з інформаційними потоками. У будь-якому випадку усі стратегічні та тактичні дії щодо проектування та впровадження сучасних систем захисту інформації вимагають системного аналізу проблеми і дослідження операцій, які супроводжуються складними інформаційними процесами, більшість з яких мають конфіденційний характер.

Особливої уваги на підприємстві приділяється інформаційним систем комплексного захисту інформації, які являють собою сукупність організаційних і технічних заходів, апаратних і програмних засобів.

Функціонування системи технічного захисту інформації здійснюється з урахуванням необхідності забезпечення гарантії відповідності рівня захищеності інформації вимогам нормативних документів. При цьому необхідну якість робіт з технічного захисту інформації можна забезпечити за умови залучення спеціалістів, які мають відповідну фахову підготовку та досвід роботи, при відповідному технічному оснащенні.

Обов’язковою умовою забезпечення захисту інформації, яка циркулює в інформаційно-телекомунікаційних системах та на об’єктах інформаційної діяльності, є одержання об’єктивної оцінки рівня захищеності інформації.

У той же час багато рішень пропонують захист в комплексі, тобто, наприклад, мережеві екрани інтегрують в собі ще й захист від вірусів, а системи виявлення і попередження вторгнень є, як правило, між мережевими екранами. Однак, напевно говорити, що дана система є між мережевим екраном, до якої було інтегровано функції системи виявлення і попередження вторгнень, або навпаки, не можна без конкретного аналізу розвитку даної системи забезпечення захисту інформації.

Організація системи захисту комп'ютерних мереж ускладнюється тим, що загрози, від яких доводиться захищати мережі та дані, дуже не визначені і носять різноманітний характер. По своєму походженню це можуть бути фактори антропогенні, технічні, технологічні, часові, природні і ін., котрі не завжди вдається прогнозувати.

Найбільш важливим засобом захисту мереж є мережеві екрани (або між мережеві екрани, файрволи чи брандмауери) та проксі-сервера.

Науковий керівник — д.т.н. Володимир Квасніков

Проблеми захисту інформації в системах автоматизованого тестування та діагностики мобільного робота

УДК 004.056
Світлана Марченкова
Національний авіаційний університет, Україна, s.marchenkova90@gmail.com

Надійність і безпека сучасних організаційних і технічних систем є важливою складовою їх якості та необхідною умовою забезпечення надійності і безпеки виробничих об'єктів. Головна мета аналізу надійності і безпеки – своєчасне отримання достовірної інформації про властивості надійності та безпеки систем, необхідної для вироблення, обґрунтування і реалізації ефективних проектних і експлуатаційних рішень.

Програмний комплекс дозволяє на основі схем функціональної цілісності (опис «правильного» функціонування об'єкта) автоматично будувати дерева відмови, які є основою для побудови систем технічної діагностики складних об'єктів управління.

National Instruments (NI) TestStand – це ПЗ для управління тестами. Воно дозволяє швидко розробляти і проводити тести електронних вузлів літаків і вертольотів. NI TestStand дозволяє об'єднати підпрограми тестування, написані в будь-якій мові програмування, включаючи графічний код LabVIEW і текстові процедури, написані в C / C + +.

Її відмінними характеристиками є наступні: 1) Графічна середа роботи з тестами; 2) Інтерфейси для виклику тестових процедур, написаних у різних мовах програмування; 3)Паралельне виконання тестових послідовностей для збільшення пропускної здібності; 4)Генерація звітів у форматах ASCII, HTML / Web, XML, ATML; 5)Інтеграція з Access, Oracle, SQL Server.

Рішення, які пропонуються NI, засновані на сучасних комп'ютерних і промислових технологіях, таких як високошвидкісні шини передачі даних PCI, PCI Express, PXI, PXI Express, USB і Ethernet, швидкі процесори, операційні системи реального часу, надійні платформи з ПЛІС, середовища графічного і текстового програмування – LabVIEW, LabWindows / CVI, Measurement Studio. Розробляючи системи на базі технологій NI, можна отримати необхідну функціональність, максимальну продуктивність і відносно швидке впровадження системи. Модульні технології обладнання і ПЗ NI дозволяють з мінімальними витратами розробляти вимірювальні системи різної конфігурації і складності: 1) Системи для проведення стендових випробувань. Багатоканальні модульні системи для вимірювання статичних і динамічних сигналів з датчиків, збереження даних на RAID-масиви та управління стендовими випробуваннями. Багатофункціональні середовища розробки і готові програми для стендових випробувань; 2) Автоматизовані системи тестування. Модульні системи PXI для проведення автоматизованих тестів бортового обладнання, авіоніки, електронних блоків, систем зв'язку та навігації. 3) Системи управління і імітатори. Технології NI для налагодження та розробки систем управління, імітаторів, а також комплексного програмно-апаратного моделювання із замкнутим циклом «Система управління – об'єкт випробувань» (рис. 1)

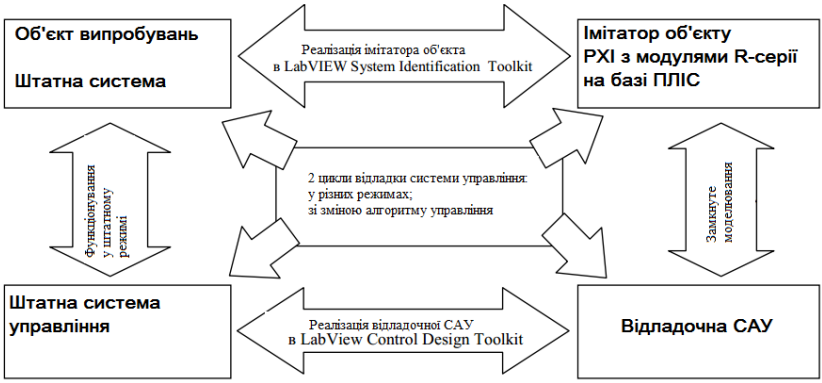

Рис. 1. – Технології NI для створення систем управління і імітаторів

Використання інструментарію LabVIEW для аналізу та обробки інформації, що надходить з МР, обумовлено простотою системи, а також можливістю її сполучення з великим числом одиниць використовуваного обладнання.

Можна виділити дві основні фази аналізу МР: 1)Аналіз стану, що проводиться на спеціальному стенді; 2) Аналіз стану, що проводиться самим МР.

У цих випадках для ефективного аналізу стану МР і наступних керуючих впливів необхідно зберігати отримані дані в сховищі, з можливістю їх подальшого відтворення та аналізу. До складу ПЗ LabVIEW входить підсистема роботи з реляційними базами даних Database Connectivity Toolset, яка надає різні механізми (ADO, ODBC тощо) доступу до систем управління базами даних.

Робота LabVIEW з СУБД має досить багатий інструментарій, що дозволяє отримувати інформацію не тільки про дані, а й про типи, збережених в таблицях, налаштуваннях таблиць, іменах полів, можливості обробки пропущених значень і багато чого іншого.

При створенні системи статистичної обробки інформації по випробуванню МР використовуються непараметричні методи обробки випадкових процесів, а в якості програмних пакетів систем обробки даних застосовані популярні предметно-орієнтовані інструментальні засоби, такі як MathCad, Matlab, Statgraphics, Statistica, NCSS, NI DIAdem.

Середа постобробки даних NI DIAdem інтегрована з різноманітним обладнанням компанії NI і забезпечує спрощення та прискорення обробки великих обсягів даних.

DIAdem – інтерактивне ПЗ NI для пошуку і управління технічними даними, математичного та інтерактивного графічного аналізу даних, а також представлення даних у вигляді звітів. Можна налаштувати інструменти під завдання і автоматизувати їх виконання за допомогою скриптів, що значно скорочує час обчислень та забезпечує захист інформації системи.

Науковий керівник — д.т.н. Володимир Кваснiков

Адаптивні методи стиснення цифрової графічної інформації

УДК 681.377

Олександр Осмоловський
Національний авіаційний університет, Україна, osmo5@ukr.net

Стрімкий розвиток цифрових технологій дозволив поступово відмовитися від більшості традиційних методів передачі, обробки та збереження інформації в аналоговій формі. Окрім текстової, числової та інших видів детермінованої інформації, для яких розроблені і використовуються достатньо ефективні методи компактного її представлення – архіватори, перетворенню в числову форму з метою подальшої обробки і збереження почали піддаватися й інші види інформації, які тривалий час не були придатні для такої процедури внаслідок занадто високих вимог до потужності існуючих комп'ютерних засобів. Мова йде про зображення, які можна представити у вигляді двовимірних масивів даних, в якості індексів елементів яких виступають координати відповідних фрагментів. Проблема ефективного стиснення цифрової інформації з метою її компактного зберігання і скорочення часу, необхідного для доступу та передачі даних, і зараз залишається актуальною.

Застосування архіваторів, призначених для текстової або числової табличної інформації, для стиснення графічної інформації у загальному випадку не є ефективним, оскільки вони не враховують специфіки цього виду даних і не можуть використати додаткові можливості для одержання кращого результату. В доповіді запропоновано методи, які дозволяють досягти підвищеного ступеня стиснення цифрової графічної інформації у порівнянні з відомими.

Специфіка цифрових зображень повністю визначається особливостям вихідного аналогового зображення. Часто для оцінки можливостей стиснення цифрового коду важливим є параметр, що визначає рівні сигналу, які він може приймати з певною ймовірністю. Граничний випадок – бінарний сигнал, коли цифровий код приймає тільки два певні значення. Проміжний випадок – індексований цифровий сигнал, за якого кількість можливих значень менша за повне число рівнів, визначених розрядністю цифрового коду.

Для тестування запропонованих методів стиснення зображень використано кілька моделей сигналів, окремі форми яких представлено на діаграмах рис. 1, 2.

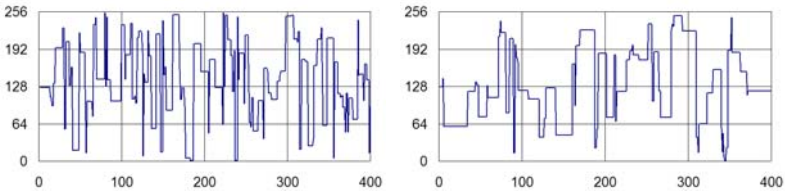

Рис. 1. Приклади відеосигналів прямокутної форми з різною частотою перемикань.

Розрахунки виконано для фрагменту монохромного зображення, представленого числовою послідовність восьмирозрядного двійкового коду довжиною у 1024 відліки. У загальному випадку дану послідовність можна записати у

вигляді прямокутної матриці двійкових однорозрядних чисел a_{ij} розміром 8 х 1024, де $i = 1…8$ – номер рядка, $j = 1…1024$ – номер стовпця матриці.

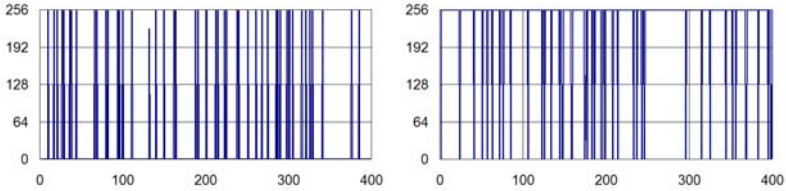

Рис.2. Приклади бінарних сигналів з різним усередненим значенням.

До елементів матриці застосовано такі перетворення: пряме, яке умовно назвемо диференціюванням однорозрядних двійкових чисел:

$$b_{1j} = a_{1j} \text{ для першого рядка}, \quad b_{ij} = \left| a_{ij} - a_{i-1,j} \right| \text{ для } i = 2…8,$$

де $j = 1…1024$, та зворотне перетворення, яке назвемо інтегруванням однорозрядних двійкових чисел:

$$a_{1j} = b_{1j} \text{ для першого рядка}, \quad a_{ij} = \left| b_{ij} - a_{i-1,j} \right| \text{ для } i = 2…8.$$

Метою перетворення є формування такого поля чисел матриці, зчитування якого дасть найменшу кількість переходів з “0” на “1” та з “1” на “0”. В роботі обгрунтовано використання окремих комбінацій таких перетворень і виконано розрахунки ефекту покращення ступеня стиснення цифрової інформації.

Найпростіший алгоритм – це послідовне зчитування стовпців матриці, що відповідає звичайному одержанню інформації байт за байтом (позначимо його як “спіраль”). Інший підхід – зчитування даних стовпців зі зміною напрямку (у формі “змійки”). До більш детального розгляду пропонується алгоритм порозрядного зчитування всього відеофрагменту, тобто по рядках вихідної матриці.

В таблиці 1 представлено порівняльні результати застосування різних алгоритмів попередньої обробки цифрових даних перед стисненням. Критерієм ефективності алгоритму обрано кількість перемикань сигналу на протязі всього відеофрагменту довжиною 8 192 біт. В якості тестових обрано різні форми сигналів, назви та параметри яких позначено в головній частині таблиці.

Таблиця 1. Оцінка ефективності стиснення

Сигнал	Відео			Шум			Бінарний		Лінійний			Лінійний з шумом		
Параметр	Період перемикань			Постійна інтегрування			Поляр-ність		Швидкість, біт/елем.			Частка шуму, %		
Знач. парам.	2	4	16	1	16	256	Поз.	Нег.	4	16	64	1	7,5	50
Оцінка потенційної ефективності стиснення, %														
До спіралі	29,9	22,0	11,0	95,7	58,8	40,2	100	100	1,4	7,6	50,1	5,7	37,1	55,9
До змійки	32,9	24,8	12,8	96,5	62,0	42,6	100	100	1,6	9,2	60,2	6,5	39,6	58,9
Абсолютна	14,7	11,0	5,5	47,2	31,4	20,8	3,6	2,6	0,6	2,4	9,4	2,5	18,7	29,3

Розглянутий підхід дозволяє досягти підвищення ступеня стиснення цифрової графічної інформації. На підставі результатів порівняльного аналізу запропонованих алгоритмів з відомими можна зробити висновок про доцільність

застосування адаптивних методів попередньої обробки графічної інформації в залежності від специфіки окремих фрагментів цифрових зображень.

Методи вимірювань деформацій і механічних напружень

Таїсія Ганєва
Одеська державна академія технічного регулювання та якості, Україна,
oc.odivt-taisiia@mail.ru

Вимірювання деформацій і механічних напруг широко застосовується при дослідженні фізичних властивостей матеріалів і міцністю випробуваннях різних деталей, машин, будівельних конструкцій і споруджень. Вимірювання деформацій використовують при технічній діагностиці, а також при вимірюванні фізичних величин (сили, моментів, тиску), які перетворяться в деформацію пружного елемента. У більшості методів вимірювання механічних напруг датчиком сприймається абсолютне або відносне значення деформації, оскільки природною вхідною величиною застосовуваних при цьому перетворювачів є переміщення. Безпосередньо вимірювати механічні напруги можна термопружним, магнітопружним, ультразвуковим і фотопружним методами.

Перехід від обмірюваних деформацій до механічних напруг можна здійснити при відомих функціональних залежностях між деформацією й напругою. При однорідному об'ємному напруженому стані ізотропного матеріалу в межах пружних деформацій можна за обмірюваними значенням головних деформацій ε_1, ε_2, ε_3, σ_1, σ_2, σ_3, користуючись рівняннями зв'язку.

За межею пружності перехід від деформацій до напруг викликає труднощі, якщо заздалегідь не відома функціональна залежність між напруженнями та деформаціями. Напруження у внутрішніх шарах досліджуваного об'єкта можна визначити за виміряними деформаціями на його зовнішній поверхні, якщо відомий закон розподілу деформацій по товщині об'єкта. У прозорих зразках або в моделях з прозорих діелектриків внутрішнє напруження можна визначити поляризаційно-оптичним методом, заснованим на фото пружному ефекті. Деформації необхідно вимірювати в досить широких межах - від сотих часток мікрометра до метрів, відносні деформації - в діапазоні 0-100% і більше. Малі деформації мають місце в металах і твердих пластмасах, великі деформації необхідно вимірювати при випробуванні зразків з великим подовженням.

Для вимірювань механічних напружень і деформацій найчастіше застосовують тензорезистори, які наклеюють на об'єкт. Металевими тензорезисторами вимірюють відносні деформації від 0,002 % до 2 %, а напівпровідниковими - до 0,1 %. Дротяними тензорезисторами, закріпленими на кінцях бази, вимірюють деформації до 6-10%. Через малу інерційність тензорезистори використовують для вимірювань змінних деформацій у діапазоні частот від 1 Гц до 100 кГц.

Оскільки механічне напруження і деформація є векторними величинами, тензорезистор має бути наклеєний на поверхню досліджуваної деталі вздовж напрямку їх дії.

При вимірюванні деформації її спочатку перетворять в переміщення кінців чутливого елемента тензометра, відстань між якими називається базою. При цьому використовуються два способи кріплення первинного перетворювача до об'єкта випробування.

У першому випадку первинний перетворювач безпосередньо зміцнюється на випробуваному об'єкті. Такий спосіб вимірювання, широко застосовуваний при комплексних випробуваннях складних об'єктів з використанням тензорезисторів, відрізняється невисокою точністю (похибка 2-10 %) внаслідок великого розкиду параметрів тензорезисторів і неможливості градувати прилад (канал) з даним тензорезистором, який при таких вимірах є елементом разового використання.

У другому випадку датчик тензометра, що включає в себе первинний перетворювач (тензорезистивний, індуктивний, електрооптичний), прикріплюється до досліджуваного об'єкта за допомогою спеціальних пристроїв, виконуваних у вигляді опорних призм, ножових щупових, пружинних, магнітних та інших типів захватів. Для вимірювань при високих температурах (до 1100 ˚С) застосовуються захвати з кварцовими наконечниками. Такі тензометри зазвичай використовують спільно з випробувальними машинами для міцності випробувань деталей, зразків матеріалів та окремих елементів складних конструкцій.

Переміщення захватів, викликане деформацією випробуваного зразка, вимірюється за допомогою різних методів і засобів вимірювань, але найбільш широко застосовуються тензорезистивні, індуктивні і електрооптичні тензометри. Тензометри, використовувані разом з випробувальними машинами, забезпечують вимірювання з відносно малими похибками (0,2-1,5%), оскільки їх можна градувати спільно з датчиком за допомогою зразкових засобів вимірювань довжини.

Для вимірювання деформацій і механічних напруг при натурних випробуваннях різних машин, конструкцій транспортних засобів та інших виробів найбільш широко використовується метод, заснований на застосуванні дискретних металевих і напівпровідникових тензорезисторів. Особливістю випробувань складних виробів є наявність великого числа точок тензометрирования, тому для цих цілей використовуються багатоканальні тензостанції і інформаційно-вимірювальна система для міцності випробувань.

Науковий керівник — д.т.н. Володимир Квасніков

Системы защиты информации в измерительных роботах

УДК 004.056

Н. В. Михалко
Национальный авиационный университет, Украина, kvp@nau.edu.ua;

Измерительные роботы – автоматические измерительные устройства, отличающиеся хорошими манипуляционными свойствами, высокими скоростями перемещений и измерений.

В мелкосерийном и среднесерийном производстве при частой сменяемости выпускаемых изделий широкое применение находят контрольно-измерительные машины: измерительные роботы и координатно-измерительные машины (КИМ). С их помощью автоматизируются процессы измерения и наладки в автоматизированных комплексах машиностроения.

Измерительные роботы могут выполнять типовые контрольные операции: качественная оценка состава рабочей среды; установление присутствия определенных объектов, их счет, определение расположения, сортировка; оценка значения параметров деталей.

Захватные устройства могут быть механическими, вакуумными, электромагнитными. Базы данных и знаний содержат информацию о последовательности действий, позициях и времени выполнения операций, набор возможных объектов, образцовых значений. Датчики d могут определять наличие объекта, его положение, регулировать усилие захватного устройства и т.д.

Измерительные роботы позволяют выполнять работы в труднодоступных (морское дно, космос и т.п.) и опасных для здоровья (запыление пространства, радиация, взрывоопасность и т.п.) местах, сократить утомительные операции и простои оборудования.

В более сложных робототехнических комплексах захватное устройство находит в строго фиксированных местах нужное измерительное средство и осуществляет качественную и количественную оценку параметров изделия.

Новые возможности для современного производства создают широкоуниверсальные, автоматические, достаточно гибкие средства контроля – координатные измерительные машины (КИМ). С их применением повышается точность и достоверность результатов измерения. Использование принципов оперативного и диалогового программирования дало возможность применения КИМ как универсального средства контроля в единичном и мелкосерийном производствах.

Таким образом, использование КИМ позволяет оперативно измерять геометрические параметры простых и сложных прецизионных деталей, включая корпусные, измерение которых традиционными способами требует дорогостоящей специальной оснастки или измерение которых невозможно вообще; сокращать время на наладку обрабатывающих станков, центров и модулей за счет быстрого и достоверного контроля первых обработанных деталей из последующей партии; исключать брак, используя постоянный контроль точности процесса обработки деталей, и своевременно корректировать его.

Науковий керівник — д.т.н. Володимир Квасніков

Захист інформації в системах діагностування

УДК 531.72 Юлія Ізбаш
Національний авіаційний університет, Україна, kvp@nau.edu.ua

Процес інтенсивного розвитку інфраструктури, об'єктів промисловості і сільського господарства на рівні ринкових відносин, ріст недержавного сектора економіки висувають на перший план проблеми технічного досягнення науки і техніки та впровадження більш досконалих технічних засобів. Їх впровадження базується на широкому використанні складних автоматизованих систем і комплексів. При цьому ставиться задача забезпечити створення і опановування серійного випуску не тільки самих технічних систем, а також автоматичних систем контролю та діагностування.

Процедура контролю полягає в перевірці відповідності якості об’єкта відповідним вимогам. Ці вимоги задаються звичайно у вигляді обмежень на показники властивостей об’єкта. Показники властивостей об’єкта, що доступні для спостереження, використовуються як ознаки для визначення виду його технічного стану, що позначаються як контролюючі ознаки. Ними можуть бути різні параметри об’єкта або деякі функції їх, зокрема вихідні сигнали об’єкта або окремих його складових частин (блоків, модулів, приладів тощо). Як правило, ці ознаки мають цілком конкретний кількісний вираз і значення їх можна виміряти чи визначити. Тому такі ознаки називають кількісними. Поряд з ними існують і якісні ознаки, які можна відрізнити за допомогою органів почуття людини (незвичайний шум працюючого механізму, надмірний нагрів окремих елементів об’єкта, запах горілої ізоляції тощо). При контролі технічних станів об’єктів, особливо дистанційно управляючих, використовуються переважно кількісні ознаки.

Для кожної такої ознаки задається інтервал, віднесений з визначеним видам технічного стану об’єкта. Якщо виміряне (або визначене іншим способом) значення ознаки знаходиться у цьому інтервалі, то відповідний йому стан об’єкта необхідно віднести до даного виду технічного стану. Таким чином, поняття «вид технічного стану» має у деякому сенсі збираюче (узагальнююче) значення: до даного виду технічного стану об’єкта відносяться всі його реальні стани, при яких спостережені значення ознак не виходять за межі встановлених для них інтервалів. Іншими словами, вид технічного стану об’єкта – це підмножина таких його станів, про які може бути прийняте одне і те ж рішення, узгоджене з ціллю проведеного контролю.

Стан об’єкта являє собою набір таких змінних (змінні стани), які хоч і повністю визначають положення об’єкта як абстрактної динамічної системи у деякому просторі у визначений момент часу, але самі по собі не дозволяють встановити, правильно чи функціонує об’єкт і чи справний він. Для того щоб винести таке судження, необхідно порівняти кожну змінну стану об’єкта з деяким конкретним еталонним значенням.

Таким чином встановлюється в даний момент стан об’єкту справним чи несправним, працездатним чи непрацездатним, правильно функціонуючим чи неправильно функціонуючим тощо.

Современная криптографія

УДК 004.056(043.2)

Гульнур Жангисина, Рахиля Мырзаш,
Барат Капия, Бакберген Жолымбет
Казахский национальный технический университет им. К.И. Сатпаева,
Казахстан, gul_zhd@mail.ru

В современном мире знания о методах шифрования, о возможностях криптографии, математических методах обеспечения конфиденциальности и аутентичности (целостности и подлинности авторства) информации очень важна рядовому пользователю компьютера и компьютерных систем. Элементы современной криптографии нужны также и для руководителей организаций для того, чтобы уметь засекретить важную достоверную информацию от утечки ее по каналам связи! В современных условиях стремительного развития компьютерных технологий именно информационная безопасность очень важна, так как квалифицированная защита ее будет способствовать защите государственной независимости.

С конца 1990 годов начинается процесс открытого формирования государственных стандартов на криптографические протоколы. Пожалуй, самым известным является начатый в 1997 году конкурс AES, в результате которого в 2000 году государственным стандартом США для криптографии с секретным ключом был принят шифр Rijndael, сейчас уже более известный как AES. Аналогичные инициативы носят названия NESSIE (англ. New European Schemes for Signatures, Integrity, and Encryptions) в Европе и CRYPTREC (англ. Cryptography Research and Evaluation Committees) в Японии.

В самих алгоритмах в качестве операций, призванных затруднить линейный и дифференциальный криптоанализ кроме случайных функций (например, S-блоков, используемых в шифрах DES и ГОСТ) стали использовать более сложные математические конструкции, такие как вычисления в поле Галуа в шифре AES. Принципы выбора алгоритмов (криптографических примитивов) постепенно усложняются. Предъявляются новые требования, часто не имеющего прямого отношения к математике, такие как устойчивость к атакам по сторонним каналам. Для решения задачи защиты информации предлагаются всё новые механизмы, в том числе организационные и законодательные. Также развиваются принципиально новые направления. На стыке квантовой физики и математики развиваются квантовые вычисления и квантовая криптография. Хотя квантовые компьютеры лишь дело будущего, уже сейчас предложены алгоритмы для взлома существующих «надёжных» систем (например, алгоритм Шора). С другой стороны, используя квантовые эффекты, возможно построить и принципиально новые способы надёжной передачи информации. Активные исследования в этой области идут с конца 1980-х годов. В современном мире криптография находит множество различных применений. Кроме очевидных — собственно, для передачи информации, она используется в сотовой связи, платном цифровом телевидении при подключении к Wi-Fi и на транспорте для защиты билетов от подделок, и в банковских операциях, и даже для защиты электронной почты от спама.

История криптографии насчитывает несколько тысячелетий. Первые письменные источники относятся к 1900-м годам до н. э. Именно этим периодом датируются найденные в Египте свитки, в которых использованы видоизмененные иероглифы, по-видимому применявшиеся для конфиденциального обмена сведениями.

Хрестоматийным является пример криптографии в Древней Греции, относящийся к V в. до н. э. Во время войны Спарты против Афин для передачи военных донесений использовался так называемый шифр «Сцитала». «Сцитала» представляла собой цилиндрический жезл, на который без нахлестов и разрывов наматывалась узкая полоска папируса или пергамента. Текст записывался вдоль оси «Сциталы», а затем лента снималась с жезла. В результате получались беспорядочно написанные буквы. Адресат для прочтения сообщения использовал такую же «Сциталу». Множество шифров известно из художественной литературы, например «Пляшущие человечки» Конан-Дойля, зашифрованное послание в «Золотом жуке» Эдгара По, криптограмма в «Путешествии к центру Земли» Жюля Верна. Все они были достаточно просты и не представляли особой сложности для квалифицированного человека (как следует из тех же литературных произведений). Но ручные способы шифрования, пригодные в частной переписке, были не очень удобны в условиях, когда количество секретной информации достаточно велико, например в военное время. Эта проблема вызвала к жизни шифровальные машины, наиболее известной из которых является немецкая Enigma («Загадка»), использовавшаяся фашистской Германией во Второй мировой войне. Появление шифровальных машин дало толчок и развитию компьютеров, поскольку первые из них (например, британский Colossum) создавались специально для вскрытия шифров. С развитием телекоммуникаций встал вопрос защиты не только отдельных сообщений, но и непрерывного потока передаваемых данных (например, телефонного разговора). Все это вызывало разработку и появление все новых и новых шифров. Но несмотря на все их многообразие, их достаточно легко классифицировать по нескольким основным типам. Криптография– наука о математических методах обеспечения конфиденциальности (невозможности прочтения информации посторонним) и аутентичности (целостности и подлинности авторства) информации. Другими словами, криптография изучает методы шифрования информации, то есть способы защиты данных, применяемые для хранения критически важной информации в ненадежных источниках или передачи ее по незащищенным каналам связи. Шифрование как процесс своей историей уходит глубоко в века. Так, подстановочные шифры существуют уже около 2500 лет. Яркий тому пример – шифр Атбаш, который возник примерно в 600 году до нашей эры. Суть его работы заключалась в использовании еврейского алфавита в обратном порядке. Юлий Цезарь также использовал подстановочный шифр, который и был назван в его честь – шифр Цезаря. Суть шифра Цезаря заключалась в том, чтобы заменить каждую из букв другой, стоящей в алфавите, на три места дальше от исходной. Так, буква А превращалась в Д, Б преобразовывалась в Е, Я преобразовывалась в Г и т. д. Шифрование можно назвать одним из важнейшим средств обеспечения безопасности. Однако не следует забывать и о том, что само по себе шифрование отнюдь не панацея от всех проблем. Механизмы шифрования могут и должны являться составной частью комплексной программы по обеспечению безопасности.

Согласно классическим канонам Информационной безопасности с помощью шифрования обеспечиваются три основополагающих состояния безопасности информации.

1) Конфиденциальность. Шифрование используется для сокрытия информации от неавторизованных пользователей при передаче или хранении.

2) Целостность. Шифрование используется для предотвращения изменения информации при передаче или хранении. Яркий пример – контрольная сумма, полученная с

использованием хэш-функции (то, что можно увидеть на FTP-серверах рядом с файлом (примерно так – dpofgj 0 93utm34tdfgb45ygf), который собираемся скачать).

3) Идентифицируемость. Шифрование используется для аутентификации источника информации и предотвращения отказа отправителя информации от того факта, что данные были отправлены именно им.

Известно, что любая система шифрования может быть взломана. Речь идет лишь о том, что для получения доступа к защищенной шифрованием информации может потребоваться неприемлемо большое количество времени и ресурсов. Что это значит и как это выглядит в реальной жизни? Представьте себе такую ситуацию: злоумышленнику каким-то образом удалось перехватить зашифрованную информацию. Дальнейшие действия взломщика могут быть сведены к двум вариантам взлома (возможен и третий, который сводится к эксплуатации уязвимостей рабочей среды): 1) атака "грубой силой", или Brute Force (атаки "грубой силой" подразумевают подбор всех возможных вариантов ключей); 2) поиск уязвимых мест в алгоритме.

Учитывая тот факт, что применяемые в настоящее время алгоритмы шифрования уже проверены "огнем и временем", совершенно очевидно, что взломщик будет использовать Brute Force. Взлом конфиденциальной информации, зашифрованной стойким алгоритмом и достаточно длинным ключом (к примеру, 512 бит), потребует со стороны взломщика использования "армии" суперкомпьютеров или распределительной сети из нескольких сотен тысяч машин плюс уйму времени и денег. Но если деньги есть, то почему бы и нет! Современная криптография основана на понятии односторонней функции f(x). Не вдаваясь в формальные математические определения, отметим одно ее свойство: инвертировать функцию, т. е. вычислить x, зная только f(x), крайне сложно (на строгий язык математики слова «крайне сложно» переводятся в виде трех абзацев текста, набитых формулами, которыми не стоит утомлять читателя). Расширением этого понятия является функция с ключом, в которой к x добавляется секретный элемент K. Забавно, но существование односторонних функций до сих пор не доказано. Равно как и их отсутствие. Существует только предположение, что некоторые из известных функций могут оказаться односторонними, и именно они используются в современных схемах шифрования. Некоторую уверенность в правильном выборе этих функций дает тот факт, что их инвертирование эквивалентно сложным математическим задачам, которые изучаются уже многие годы и для которых не найдено эффективного решения (помимо полного перебора). Одна из этих задач по формулировке весьма проста — найти разложение числа на сомножители. Если в качестве примера выбрать простые числа приблизительно равной и достаточно большой величины, то современная математика не даст практически никаких рецептов решения, за исключением полного перебора. Второй задачей является дискретное логарифмирование, т. е. инвертирование функции $F(x) = ax \bmod p$, где p — простое число. Кстати, на этой формуле зиждется известная схема шифрования RSA, названная так по первым буквам фамилий ее изобретателей.

В зависимости от используемых ключей шифрование условно можно разделить на следующие виды: 1) Симметричное шифрование, при котором ключ для шифрования и дешифрования представляет собой один и тот же ключ (на обыденном уровне – просто пароль). 2) Асимметричное шифрование: подразумевает использование двух различных ключей – открытого и закрытого. Открытый ключ, как правило, передается в открытом виде, закрытый же всегда держится в тайне. Стойкость шифров, помимо собственно ал-

горитма шифрования, во многом определяется и длиной ключа. Современная криптография исходит из того, что сам алгоритм рано или поздно все равно станет известен противнику. Все сообщения, передаваемые по открытым каналам связи, могут быть перехвачены, так что ключ шифра остается его единственным секретом. Американский стандарт симметричного шифрования DES использует длину ключа 56 бит, что дает 255 вариантов ключей. Казалось бы, огромное количество — несколько десятков квадрильонов! Но мощь современных компьютеров такова, что последний раз DES был вскрыт три года назад (19 января 1999 г.) за 22 ч 15 мин. В настоящее время симметричный шифр считается стойким, только если длина его ключа не менее 128 бит.

Каждый пользователь ПЭВМ должен знать и уметь пользоваться методами шифрования своей конфиденциальной информации. В системе образования также необходимы курсы повышения педагогов по информационной безопасности.

Защита информации

УДК 004.056(043.2)

Гульнур Жангисина, Арай Алиева, Нурсанат Аскарова, Айгерим Елибаева, Куляш Турмагамбетова
Казахский национальный технический университет им. К.И. Сатпаева, Казахстан, gul_zhd@mail.ru

Защита любой информации является важным научным направлением в современных условиях развития Международного сотрудничества, усиления угрозы безопасности в глобальном пространстве. Следует отметить, что нет универсальной методики, которая позволяла бы четко соотносить ту или иную информацию к категории коммерческой тайны. Обычно исходят из принципа экономической выгоды и безопасности предприятия - чрезмерная "засекреченность" приводит к необоснованному подорожанию необходимых мер по защите информации и не способствует развитию бизнеса, когда как широкая открытость может привести к большим финансовым потерям или разглашению тайны. Безопасность проявляется как невозможность нанесения вреда функционированию и свойствам объекта, либо его структурных составляющих. Это положение служит методологическим основанием для выделения видов безопасности. Одной из важных структурных составляющих многих объектов безопасности является информация или деятельность, предметом которой является сама информация. Наличие угроз этим объектам позволяет говорить об их информационной безопасности — безопасности их "информационного измерения". Объектом информационной безопасности может быть коммерческое предприятие(а также и некоммерческое!). Тогда содержание "информационной безопасности" будет заключаться в защищенности интересов собственника данного предприятия, удовлетворяемых с помощью информации, либо связанных с защитой от несанкционированного доступа тех сведений, которые представляются собственнику достаточно важными. Интересы проявляются через объекты, способные служить для их удовлетворения, и действия, предпринимаемые для обладания этими объектами. Соответственно интересы как объект безопасности могут быть представлены совокупностью информации, способной удовлетворять интерес собственника, и его действий, направленных на овладение информацией или сокрытие информации. Эти составляющие объекта информационной безопасности и защищаются от внешних и внутренних угроз. В случае, когда собственник предприятия не видит необходимости в защите своих действий, например, в

связи с тем, что это не окупается, содержание информационной безопасности предприятия может быть сведено к защищенности конкретной информации, раскрытие которой может принести заметный ущерб коммерческой деятельности. Подобную информацию обычно относят к коммерческой тайне.

Объектом информационной безопасности в определенных случаях может быть информационная система. Тогда под информационной безопасностью будет пониматься "защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, чреватых нанесением ущерба владельцам или пользователям информации и поддерживающей инфраструктуры". Вследствие этого правильный с методологической точки зрения подход к проблемам обеспечения информационной безопасности должен начинаться с выявления субъектов отношений, связанных с использованием информационных систем. Спектр их интересов может быть разделен "на следующие основные категории: доступность (возможность за приемлемое время получить требуемую информационную услугу), целостность (актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения), конфиденциальность (защита от несанкционированного ознакомления)". Построение надежной защиты включает оценку циркулирующей в информационной системе информации с целью уточнения степени ее конфиденциальности, анализа потенциальных угроз ее безопасности и установление необходимого режима ее защиты. Законом "О Концепции информационной безопасности Республики Казахстан" определено, что информационные ресурсы, т.е. отдельные документы или массивы документов, в том числе и в информационных системах, являясь объектом отношений физических, юридических лиц и государства, подлежат обязательному учету и защите, как всякое материальное имущество собственника. При этом собственнику предоставляется право самостоятельно в пределах своей компетенции устанавливать режим защиты информационных ресурсов и доступа к ним. Закон также устанавливает, что "конфиденциальной информацией считается такая документированная информация, доступ к которой ограничивается в соответствии с законодательством Республики Казахстан". При этом закон может содержать прямую норму, согласно которой какие-либо сведения относятся к категории конфиденциальных или доступ к ним ограничивается. Так, закон "О Концепции информационной безопасности Республики Казахстан" напрямую относит к категории конфиденциальной информации персональные данные (информацию о гражданах).

Однако не ко всем сведениям, составляющим конфиденциальную информацию, применима прямая норма: соответствующая информация неизвестна третьим лицам; к ней свободного доступа на законном основании; меры по обеспечению ее конфиденциальности принимает собственник информации.

Закон "О Концепции информационной безопасности Республики Казахстан", определяя нормы, согласно которых сведения относятся к категории конфиденциальных, устанавливает и цели защиты информации: предотвращение утечки, хищения, искажения, подделки информации; предотвращение несанкционированных действий по уничтожению, искажению, блокированию информации; сохранение государственной тайны, конфиденциальности документированной информации.

Но основной целью информационной безопасности является предотвращения ущерба ее деятельности за счет разглашения, утечки и несанкционированного доступа к источникам информации, содержащей закрытые сведения.

Целями информационной безопасности являются:

1) Соблюдение конфиденциальности информации ограниченного доступа.

2) Предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к такой информации.

3) Предотвращение несанкционированных действий по уничтожению, модификации, копированию, блокированию и предоставлению информации, а также иных неправомерных действий в отношении такой информации.

4) Реализация конституционного права граждан на доступ к информации.

5) Недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование.

Под информационной безопасностью будем понимать состояние защищенности информационных ресурсов, технологий их формирования и использования, а также прав субъектов информационной деятельности. Здесь важно отметить следующее: объектом защиты становится не просто информация как некие сведения, а информационный ресурс (далее ИР), т.е. информация на материальных носителях (документы, базы данных, патенты, техническая документация и т.д.), право на доступ, к которой юридически закреплено за ее собственником и им же регулируется; информационная безопасность пользователей в отличие от физической обеспечивает защищенность их прав на доступ к ИР для удовлетворения своих информационных потребностей; с точки зрения экономической целесообразности защищать следует лишь ту информацию, разглашение (утечка, потеря и т.д.) которой неизбежно приведет к материальному и моральному ущербу, а также к жертвам. Злоумышленные действия над информацией не только не сокращаются, а имеют достаточно устойчивую тенденцию к росту. Опыт показывает, что для успешного противодействия этой тенденции необходима стройная и управляемая система обеспечения безопасности информации (далее ОБИ). Поскольку информация является продуктом информационной системы (ИС), т.е. организационно-упорядоченной совокупности информационных ресурсов, технологических средств, реализующих информационные процессы в традиционном или автоматизированном режимах для удовлетворения информационных потребностей пользователей, то материальными объектами информационной безопасности являются элементы таких ИС, как потребители и персонал, материально-технические средства (далее МТС) информатизации, ИР с ограниченным доступом. В связи с этим, считает, что в школах необходимо ввести спецкурсы по защите информации.

Информационная безопасность авиакомпании

УДК 004.056(043.2)

Гульнур Жангисина, Нурболат Шалаханов, Чигиз Есетов, Ринат Павликов, Ажар Сагымбекова, Кенже Каден
Казахский национальный технический университет им. К.И. Сатпаева, Казахстан, gul_zhd@mail.ru

Безопасность государства, в первую очередь, зависит от безопасности транспортных систем. Среди транспортных систем (авиация, Метрополитен, железнодорожный и авто-

дорожный транспорт, водный транспорт) особую роль играет авиация. Еще в период 2-й мировой войны весь мир убедился, что победило то государство, воздушный транспорт которого был сильнее!

Поэтому в статье мы рассматриваем проблемы информационной безопасности авиационного транспорта. Основными требованиями к информационной безопасности фирмы являются:

- обеспечение защиты информации, содержащей закрытые сведения;
- организация работы по правовой, организационной и инженерно-технической (физической, аппаратной, программной и математической) защите информации, содержащей закрытые сведения;
- организация специального делопроизводства, исключающего несанкционированное получение информации, содержащей закрытые сведения;
- предотвращение необоснованного допуска и доступа к информации, содержащей закрытые сведения;
- выявление и локализация возможных каналов утечки закрытой информации в процессе повседневной производственной деятельности и в экстремальных (аварийных, пожарных и др.) ситуациях;
- обеспечение режима информационной безопасности при проведении всех видов деятельности, включая, различные встречи, переговоры, совещания, связанные с деловым сотрудничеством, как на национальном, так и на международном уровне;
- обеспечение охраны зданий, помещений, оборудования, продукции и технических средств обеспечения информационной безопасности;
- обеспечение личной безопасности руководства и ведущих специалистов и сотрудников;
- оценка маркетинговых ситуаций и неправомерных действий злоумышленников и конкурентов.
- организует и обеспечивает пропускной и внутриобъектовый режим в зданиях и помещениях, порядок несения службы охраны, контролирует соблюдение требований режима сотрудниками;
- руководит работами по правовому и организационному регулированию отношений по защите закрытой информации;
- участвует в разработке основополагающих документов с целью закрепления в них требований обеспечения безопасности и защиты закрытой информации;
- разрабатывает и осуществляет совместно с другими подразделениями мероприятия по обеспечению с документами, содержащими закрытую информацию, при всех видах работ, организует и контролирует выполнение требований инструкции по защите информации, содержащей закрытые сведения;
- изучает все стороны производственной, коммерческой, финансовой и другой деятельности для выявления и закрытия возможных каналов утечки закрытой информации;
- организует и проводит служебные расследования по фактам разглашения закрытой информации;
- разрабатывает, ведет, обновляет и пополняет перечень информации, содержащей закрытые сведения, и другие нормативные акты, регламентирующие порядок обеспечения безопасности и защиты информации;
- обеспечивает строгое выполнение требований нормативных документов по защите информации;

- осуществляет руководство службами и подразделениями безопасности авиакомпаний по защите информации;
- организует и регулярно проводит учебу сотрудников службы безопасности по всем направлениям защиты информации, добиваясь, чтобы к охране закрытых сведений был глубоко осознанный подход;
- ведет учет сейфов, металлических шкафов, специальных хранилищ и других помещений, в которых разрешено постоянное или временное хранение закрытой информации;
- ведет учет выделенных для конфиденциальной работы помещений, технических средств в них, обладающих потенциалам утечки информации.

Сотрудники службы безопасности авиакомпании в целях обеспечения защиты закрытых сведений, имеют право:
- требовать от всех сотрудников строго и неукоснительного выполнения требований нормативных документов или договорных обязательств по защите закрытых сведений;
- вносить предложения по совершенствованию правовых, организационных и инженерно-технических мероприятий по защите информации.

Обязаны:
- осуществлять контроль за соблюдением инструкции по защите информации;
- докладывать руководству о фактах нарушения требований нормативных документов по защите информации и других действиях, могущих привести к утечке конфиденциальной информации или утрата документов;
- не допускать неправомерного ознакомления с документами и материалами, содержащими закрытые сведения, посторонних лиц.

Сотрудники службы безопасности авиакомпании несут ответственность за личное нарушение безопасности информации, содержащей закрытые сведения и за неиспользование своих прав при выполнении функциональных обязанностей по защите закрытой информации сотрудниками предприятия [9].

Средства или инструменты, с помощью которых возможно достижение целей информационной безопасности.

Перечислим основные средства (инструменты) информационной безопасности:
- персонал – люди, которые будут обеспечивать претворение в жизнь информационной безопасности во всех аспектах, то есть разрабатывать, внедрять, поддерживать, контролировать и исполнять;
- нормативное обеспечение – документы, которые создают правовое пространство для функционирования информационной безопасности;
- модели безопасности – схемы обеспечения информационной безопасности, заложенные в данную конкретную информационную систему или среду;
- криптография – методы и средства преобразования информации в вид, затрудняющий или делающий невозможным несанкционированные операции с нею (чтение и/или модификацию), вместе с методами и средствами создания, хранения и распространения ключей – специальных информационных объектов, реализующих эти санкции (симметричное/ассиметричное, поточное/блочное шифрование);
- антивирусное обеспечение – средство для обнаружения и уничтожения зловредного кода (вирусов, троянских программ и т. п.);
- межсетевые экраны – устройства контроля доступа из одной информационной сети в другую;

- сканеры безопасности – устройства проверки качества функционирования модели безопасности для данной конкретной информационной системы;
- системы обнаружения атак – устройства мониторинга активности в информационной среде, иногда с возможностью принятия самостоятельного участия в указанной активной деятельности;
- резервное копирование – сохранение избыточных копий информационных ресурсов на случай их возможной утраты или повреждения;
- дублирование (резервирование) – создание альтернативных устройств, необходимых для функционирования информационной среды, предназначенных для случаев выхода из строя основных устройств;
- аварийный (кризисный) план – набор мероприятий, предназначенных для претворения в жизнь, в случае если события происходят или произошли не так, как было предопределено правилами информационной безопасности;
- обучение пользователей – подготовка активных участников информационной среды для работы в условиях соответствия требованиям информационной безопасности.

Изложенные функции организационных структур и сложность решаемых задач по обеспечению безопасности коммерческой тайны объективно вызывают потребность использования средств вычислительной техники. В качестве конкретных решений может быть рекомендовано использование организационно-функциональных автоматизированных мест должностных лиц службы безопасности . На первом этапе внедрения средств автоматизации возможна разработка автоматизированных рабочих местов (далее АРМ) для начальника службы безопасности; для группы обработки документов с грифом "Закрытые сведения" специального отдела; для инженерно-технической группы, а в некоторых случаях для группы анализа внешней деятельности и группы режима и работы с персоналом.

На последующих этапах масштабы внедрения средств автоматизации могут быть расширены в направлении обеспечения оперативного управления текущей деятельностью служба безопасности (далее СБ) в зависимости от изменения условий.

1 Общие положения.

Служба безопасности является самостоятельным структурным подразделением фирмы и подчиняется непосредственно ее руководителю.

Служба безопасности в своей деятельности руководствуется следующими принципами: соблюдение законности, эффективность (результативность) в работе, защита законных прав клиентов, следование общепризнанным этическим нормам, конфиденциальность, плановость.

Целью деятельности СБ является своевременное выявление и нейтрализация внешних и внутренних угроз экономическому благосостоянию фирмы.

2 Основные задачи.

Обеспечение сохранности физических носителей информации, содержащих в себе закрытые сведения (документов, изделий, материалов).

Предотвращение утечки закрытой информации в процессе деятельности фирмы.

Своевременное доведение до определенного руководителем фирмы круга исполнителей классифицированных документов и сведений, которые им необходимы для выполнения служебных заданий.

Своевременная и качественная подготовка информации о режиме безопасности (состояние, перспективы и т.п.) для руководителя фирмы, принимающего решение по этим вопросам.

Обеспечение физической сохранности имущества фирмы и документов, связанных договором с фирмой.

Получение аналитическим и информационно-поисковым путем информации о конкурентах фирмы и ее клиентах, связанных договором с фирмой.

Защита от экономического (промышленного) шпионажа.

3 Функции.

Проектирование, монтаж и эксплуатационное обслуживание средств охранно-пожарной сигнализации.

Консультирование и подготовка рекомендаций клиентам по вопросам правомерной защиты от противоправных посягательств.

Обеспечение порядка в местах проведения массовых мероприятий.

Изучение деятельности фирмы, открытой информации о конкурирующих фирмах, для своевременного внесения предложений по разработке и корректировке перечня сведений, составляющих коммерческую тайну; после утверждения руководителем этого перечня незамедлительное ознакомление с ним исполнителей закрытых работ в части, касающейся их.

Осуществление контроля за правильностью засекречивания и рассекречивания работ, документов, изданий, материалов.

Оценка классифицированных документов с точки зрения предотвращения включения в них излишних данных.

Подготовка списка лиц, имеющих право классифицировать информацию.

Составление плана размещения и ведение учета помещений, в которых руководителем после соответствующей аттестации разрешено постоянное или временное хранение носителя конфиденциальной информации, а также проведение закрытых работ.

Составление и корректировка списка лиц, которые могут быть допущены к закрытым сведениям, необходимым им для выполнения служебных обязанностей.

Разработка разрешительной системы доступа сотрудников и командированных к носителям охраняемых сведений и определение места выполнения работ с ними, систематический анализ эффективности этой системы.

Принятие мер, исключающих разглашение охраняемой информации фирмы, в процессе контроля оформления документов, предназначенных для передачи заказчику, отправки и вывоза за границу, переписки с инофирмами.

Организация и ведение закрытого делопроизводства, размножение документов, содержащих экономические секреты, их учет, хранение, выдача исполнителям работ, уничтожение.

Участие в разработке мер по обеспечению безопасности при обработке сведений, составляющих коммерческую тайну, различными техническими средствами и системами, при пользовании ЭВМ.

Планирование и осуществление режимных мероприятий при проведении всех видов работ, в которых используется закрытая информация, классифицированные носители.

Содействие руководителям подразделений фирмы в разработке и осуществлении мер защиты сведений в процессе научной, конструкторской, производственной, коммерческой и иной деятельности.

Организация и проведение защитных мероприятий при испытаниях, хранении, транспортировке, уничтожении продукции, содержащей коммерческую тайну.

Разработка и осуществление мер по предупреждению утечки информации при оформлении материалов, предназначенных к опубликованию в открытой печати, для использования на конференциях, выставках, в рекламной деятельности, а также при проведении совещаний, конференций, выставок на территории объекта и вне его.

Систематический контроль за соблюдением правил обращения с носителями конфиденциальной информации на рабочих (выделенных) местах, их движением, возвратом, размножением и уничтожением.

Разработка положений, инструкций, правил и т.п. по обеспечению режима работы для исполнителей закрытых работ, специалистов своей службы безопасности.

Осуществление комплекса профилактических мероприятий по предупреждению правонарушений (уголовных, административных и гражданских) на территории фирмы.

Организация обучения лиц, допущенных к закрытым работам, проверки их уровня режимной подготовки.

Организация работ по повышению квалификации сотрудников службы безопасности (в т.ч. с привлечением приглашенных специалистов).

Организация и контроль состояния пропускного и внутри - объектового режима.

Участие в подборе лиц, планируемых для работы с представителями инофирм, проведение их инструктажа.

Организация разграничения обязанностей по защите государственной конфиденциальной информации (в случае выполнения закрытых заказов).

4 Права и обязанности.

Права:

Открытие текущих и расчетных счетов.

Внесение предложений о запрещении ведения работ с документами и изданиями, содержащими закрытые сведения, при отсутствии необходимых условий, гарантирующих информационную безопасность фирмы.

Ходатайство об отстранении конкретных исполнителей фирмы от ведения определенных работ в связи с допущенными ими нарушениями правил безопасности или о привлечении их к дисциплинарной или материальной ответственности.

Контроль (с привлечением специалистов) состояния и надежности защиты закрытых работ во всех подразделениях.

Внесение в рамках своей компетенции руководителям подразделений, исполнителям закрытых работ рекомендаций, обязательных для выполнения, приостановление информирования по закрытым вопросам сотрудников фирмы и командированных, если предоставляемые сведения выходят за рамки решаемых ими задач. Направление руководству фирмы предложений по совершенствованию режима, изменению перечня сведений, составляющих конфиденциальную информацию, и другим вопросам безопасности фирмы.

Разработка предложений по изменению организационной структуры СБ.

Обязанности:

Заключение с каждым из своих клиентов письменного договора.

Предоставление клиенту письменного отчета о результатах проделанной работы.

Совершение действий, предусмотренных законодательством.

Систематическое обучение персонала правилам и мерам безопасности.

Проведение расследований по фактам разглашения закрытой информации, утраты документов и изделий, содержащих конфиденциальную информацию, а также грубых нарушений установленных правил безопасности фирмы.

Принятие мер к восстановлению нарушенных персоналом СБ законных интересов и прав граждан и юридических лиц.

5 Руководство.

Начальник СБ назначается руководителем фирмы и подотчетен только ему.

Организационная структура СБ представляется ее начальником на утверждение руководителю фирмы.

Передача указаний, распоряжений, приказов и т.д., минуя непосредственного начальника, допускается в исключительных случаях, которые должны быть оговорены в должностных инструкциях.

Весь персонал СБ руководствуется в своей деятельности должностными инструкциями, согласованными с руководителем фирмы.

6 Взаимоотношения и связи.

С руководителем фирмы.

Получает: устные и письменные распоряжения, должностные инструкции, разрешение на приобретение специальных средств, оружия и боеприпасов, помещения с необходимым оборудованием.

Представляет: отчеты установленного образца, рапорта, докладные записки.

С главной бухгалтерией.

Получает: ведомости по уплате денежных сумм с соответствующей суммой валюты.

Представляет: закрытые ведомости о выдаче сотрудникам СБ денег, табели учета рабочего времени, копии служебных расследований по вычетам из зарплаты сотрудников, копии решений судов по гражданским делам.

С отделом кадров.

Получает: копии приказов по личному составу и по фирме.

Представляет: материалы служебного расследования в отношении сотрудников, утвержденные руководителем фирмы, заполненную анкету кандидата для работы в СБ, проверочные материалы на него, докладные записки о поощрении сотрудников, копии отчетов клиенту о результатах проделанной работы (подлежат хранению в течение 3 лет).

С клиентом.

Получает: письменный договор на оказание услуг.

Представляет: письменный отчет о результатах проделанной работы, уточненный расчет гонорара и расходов СБ.

С правоохранительными органами.

Получает: официальные документы (в рамках их компетенции) и информацию о совершенных правонарушениях и правонарушителях, необходимость которой устанавливают правоохранительные органы.

Представляет: сообщения о совершенных правонарушениях, служебную документацию (по требованию указанных в законе должностных лиц и в рамках установленных для них полномочий).

7 Охранная и детективная деятельность.

В процессе деятельности допускается:

- устный опрос граждан и должностных лиц (с их согласия);
- наведение справок;
- изучение предметов и документов (с письменного согласия их владельцев);
- внешний осмотр строений, помещений и других объектов;
- наблюдение;
- использование видео-, аудиозаписи, кинофотосъемки, технических и иных средств (не причиняющих вреда жизни и здоровью граждан и окружающей среде), а также средств оперативной радио- и телефонной связи;
- использование специальных средств и оружия (в установленном законом порядке);
- использование сторожевых собак.

В процессе деятельности запрещается:

- осуществлять какие-либо оперативно-розыскные действия, отнесенные законом к исключительной компетенции органов дознания;
- совмещать деятельность персонала с государственной службой либо выборной оплачиваемой должностью в общественных объединениях.

8 Имущество и средства.

Служебные помещения.

Мебель.

Канцелярские принадлежности.

Средства связи.

Специальные средства.

Оружие и боеприпасы.

Фотокинотехника.

Медикаменты.

Форменное обмундирование (только для охранников).

Охранно-пожарная сигнализация.

Сторожевые собаки.

Служебная документация.

Стрелковый тир, стрельбище (по разрешению органа внутренних дел).

Нормативные акты, юридическая литература.

9 Контроль, проверка и ревизия деятельности.

Контроль за служебной деятельностью СБ осуществляют руководитель фирмы и службы, уполномоченные на это (в соответствии с должностными инструкциями) сотрудники, работники органов внутренних дел и прокуратуры.

Финансовая ревизия СБ осуществляется специально созданной приказом руководителя фирмы ревизионной комиссией по утвержденному им графику.

Требования вышеуказанных лиц в рамках их компетенции о предоставлении соответствующих документов, письменной или устной информации персоналом СБ выполняются неукоснительно.

Документация по реализации контрольных функций хранится в концентрированном виде у начальника СБ.

10 Реорганизация и ликвидация.

Реорганизация допускается только в соответствии с приказом руководителя фирмы.

Ликвидация допускается по инициативе руководства фирмы и (или) в случае аннулирования органом внутренних дел лицензии. В случае ликвидации СБ приказом руководителя фирмы создается ликвидационная комиссия, которая представляет ему на утверждение акт. Не допускается ущемления законных прав персонала при реорганизации или ликвидации СБ .

Обеспечение информационной безопасности авиакомпании

Угрозы защиты информации делятся на естественные, искусственные и непреднамеренные угрозы. Угроза – это потенциальные или реальные действия, приводящие к моральному или материальному ущербу.

1.Естественные:

1) Стихийные бедствия, природные явления (пожары, землетрясения, наводнения, ураганы, смерчи, тайфуны, циклоны и т.п.).

2) Самопроизвольное разрушение элементов, из которых состоит средство электронно-вычислительной техники, электросвязи и защиты информации.

2.Непреднамеренные угрозы. Эти угрозы связаны с действиями совершаемыми людьми случайно, по незнанию, невнимательности или халатности, из любопытства, но без злого умысла:

- неумышленные действия, приводящие к частичному или полному отказу системы или разрушению аппаратных, программных, информационных ресурсов системы (неумышленная порча оборудования, удаление, искажение файлов с важной информацией или программ, в том числе системных и т.п.);
- неправомерное отключение оборудования или изменение режимов работы устройств и программ;
- неумышленная порча носителей информации;
- запуск технологических программ, способных при некомпетентном использовании вызвать потерю работоспособности системы (зависания или зацикливания) или осуществляющих необратимые изменения в системе (форматирование или реструктуризацию носителей информации, удаление данных и т.п.);
- нелегальное внедрение и использование неучтенных программ (игровых, обучающих, технологических и др. не являющихся необходимыми для выполнения нарушителем своих служебных обязанностей) с последующим необоснованным расходованием ресурсов (загрузка процессора, захват оперативной памяти и памяти на внешних носителях);
- заражение компьютера вирусами;
- неосторожные действия, приводящие к разглашению конфиденциальной информации, или делающие ее общедоступной;
- разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.);

- проектирование архитектуры системы, технологии обработки данных, разработка прикладных программ, с возможностями, предоставляющими опасность для работоспособности системы и безопасности информации;
- игнорирование организационных ограничений, при работе в системе;
- вход в систему в обход средств защиты (загрузка посторонней операционной системы с дискеты и т.п.);
- некомпетентное использование, настройка или неправомерное отключение средств защиты персоналом службы безопасности;
- пересылка данных по ошибочному адресу абонента (устройства);
- ввод ошибочных данных;
- неумышленное повреждение каналов связи.

3.Искусственные (деятельность человека):

1 Умышленные (правонарушения).

1) Пассивный (бесконтактный) несанкционированный доступ к информации:

а) визуальное наблюдение за объектами информатизации (невооруженным глазом; с помощью оптических и оптико-электронных приборов и устройств);

б) перехват речевой информации (с помощью остро направленных микрофонов, электронных стетоскопов, лазерного луча, устройств дистанционного съема речевой информации с проводных линий электросвязи, радиомикрофонных закладок, телефонных закладок, микрофонных закладок, минимагнитофонов и диктофонов);

в) электромагнитный перехват информации в радиосетях связи, побочных электромагнитных излучений, побочных электромагнитных наводок, паразитных модуляций ВЧ сигналов, паразитных информативных токов и напряжений во вспомогательных сетях технических средств передачи информации.

2) Активный (контактный) несанкционированный доступ к информации:

а) с использованием физического доступа путем непосредственного воздействия на материальные носители, иные средства обработки и защиты информации;

б) с использованием штатных и специально разработанных (приспособленных, запрограммированных) средств для негласного получения, уничтожения, модификации и блокирования информации.

2 Неумышленные (ошибки деятельности человека – непреодолимые факторы).

1) Ошибки при создании (изготовлении) средств электронно-вычислительной техники, электросвязи и защиты информации (ошибки проектирования, кодирования информации, изготовления элементов технических средств и систем);

2) Ошибки, возникающие в процессе работы (эксплуатации) средств электронно-вычислительной техники, электросвязи и защиты информации (неадекватность концепции обеспечения безопасности; ошибки управления системой защиты; ошибки персонала; сбои и отказы оборудования и программного обеспечения; ошибки при производстве пуско-наладочных и ремонтных работ.

Несанкционированное изъятие – преднамеренное или случайное изъятие (хищение, утрата) или уничтожение защищаемого актива. Возможности несанкционированного доступа способствуют различные факторы, такие как использование сетей общего доступа и расширение доступа круга пользователей, увеличение объемов информации и сосредоточение информации различного уровня важности и конфиденциальности, увеличение числа удаленных рабочих мест и автоматизация обмена информацией.

Система управління інформаційними ризиками на підприємстві «Луч»

УДК 004.4(043.2)
Людмила Кравченко
Національний авіаційний університет, Україна, lyuda.kravchenko.92@mail.ru

Розвиток науки управління ризиками в значній мірі розглядається з позиції ризиків фінансових інститутів в умовах відносно стабільної економічної кон'юнктури. Необхідність розгляду ризиків виробничих підприємств в нестабільних політичних , економічних і соціальних умовах вимагає коректування існуючих принципів управління ризиками та додаткового обгрунтування ефективності використовуваних методів аналізу ризиків . Однією з основних причин неефективного управління ризиками є відсутність ясних і чітких методологічних основ цього процесу. Аналіз приводяться в літературі принципів управління ризиками, показує їх розрізненість , а окремим спробам їх систематизації притаманні безліч спірних моментів.

Основною метою даної роботи є формування методологічних основ аналізу ризиків на підприємстві «Луч», а також формування системи управління ризиками, для забезпечення стабільної та ефективної діяльності підприємства, а також його подальшого розвитку. Для досягнення мети необхідно вирішити наступні задачі: розробити та створити систему управління інформаційними ризиками; встановити та проаналізувати всі можливі методи аналізу ризиків на підприємстві; навести основні методи зниження ризиків та розроблення механізму управління ризиками на підприємстві.

Аналіз досліджень в галузі методології управління ризиками з урахуванням вимог сучасної економіки дозволяє сформувати систему принципів управління ризиками, яка складається з наступних підходів: рішення, пов'язане з ризиком, має бути економічно грамотним і не повинно чинити негативного впливу на результати фінансово-господарської діяльності підприємства; управління ризиками має здійснюватися в рамках корпоративної стратегії організації; управління ризиками прийнятих рішень повинні базуватися на необхідному обсязі достовірної інформації; при управлінні ризиками прийняті рішення повинні враховувати об'єктивні характеристики середовища, в якій підприємство здійснює свою діяльність; - управління ризиками має носити системний характер ; управління ризиками має припускати поточний аналіз ефективності прийнятих рішень і оперативну коректуру набору використовуваних принципів і методів управління ризиками. Сутність кожного етапу управління ризиками передбачає застосування різних методів. Весь процес управління ризиками можна відобразити наступним чином: постановка цілей управління ризиками; аналіз ризику; якісний аналіз; кількісний аналіз; вибір методів впливу на ризик; аналіз ефективності прийнятих рішень та коректура цілей управління ризиками.

Етап постановки цілей управління ризиками характеризується використанням методів аналізу та прогнозування економічної кон'юнктури, виявлення можливостей і потреб підприємства в рамках стратегії і поточних планів його розвитку. На етапі аналізу ризику використовуються методи

якісного і кількісного аналізу: методи збору наявної і нової інформації, моделювання діяльності підприємства, статистичні та імовірнісні методи і т. п. На третьому етапі проводиться зіставлення ефективності різних методів впливу на ризик: уникнення ризику, зниження ризику, прийняття ризику на себе, передачі частини або всього ризику третім особам, яке завершується виробленням рішення про вибір їх оптимального набору. На завершальному етапі управління ризиками вибраних методів впливу на ризик. Результатом даного етапу має стати нове знання про ризик , що дозволяє , при необхідності, відкоригувати раніше поставлені цілі управління ризиком .

Так на кожному з етапів використовуються свої методи управління ризиками. Результати кожного етапу стають вихідними даними для подальших етапів, утворюючи систему прийняття рішень зі зворотним зв'язком. Така система забезпечує максимально ефективне досягнення цілей, оскільки знання, одержуване на кожному з етапів, дозволяє коригувати як методи впливу на ризик, так і управління ризиками. Взагалі робота була присвячена питанню організації системи управління ризиками на підприємстві. Була досягнута поставлена в роботі мета, а саме: проведення всебічних теоретичних досліджень в галузі управління ризиком на підприємстві Розглянуто теоретичні основи управління ризиком на підприємстві, наведені загальні методи зниження ризику, розроблений механізму управління ризиками підприємства в сучасних умовах господарювання.

Таким чином для ефективного аналізу всього різноманіття ризиків у діяльності підприємства необхідно застосовувати цілий комплекс методів, що, в свою чергу, підтверджує актуальність розробки комплексного механізму управління ризиками.

Науковий керівник — к.т.н. Василь Бриль

Модуль управління відносинами зі споживачем на CRM-платформі

УДК 004.056.5(043.2)
Михайло Субботін
Національний авіаційний університет,Україна,mns@e-mail.ua

Процес оперативного впровадження маркетингової ідеї управління взаємозв'язками зі споживачами викликає багато змін у звичних для українського бізнесу схемах маркетингового впливу, методах дослідження ринку та бізнес-процесах, які впливають на збільшення долі клієнтів конкретного підприємства. Тенденція сьогодення полягає в інформатизації виробничих бізнес-процесів та бізнес-процесів, пов'язаних з наданням послуг. В першу чергу оцифрування торкнулося безпосередньо основної діяльності компаній, але швидкий розвиток інформаційних технологій сприяв оцифруванню всіх видів діяльності підприємств. Оскільки конкуренція у бізнесі зростає з кожним роком, актуальним є розробка нових підходів до управління відносинами зі споживачами.

Метою даної роботи є розробка модуля автоматизації управління відносинами зі споживачем. Для досягнення поставленої мети було проведено

дослідження інформаційних систем з управління взаємозв'язками з клієнтами – CRM-системи (Customer Relationship Management). Такий інструмент управління є направленою на побудову стійкого бізнесу концепцією та бізнес-стратегією, ядром якої є клієнто-орієнтований підхід. Стратегія CRM заснована на використанні управлінських та інформаційних технологій, за допомогою яких компанія збирає інформацію про своїх клієнтів на всіх стадіях їх життєвого циклу від залучення та утримання до програм лояльності, вилучає з нього інформацію та використовує її в інтересах свого бізнесу для побудови взаємовигідних взаємовідносин. Результатом застосування CRM є збільшення конкурентоспроможності та прибутку, тому що відносини, побудовані на основі персоніфікованого підходу, дозволяють залучати нових клієнтів та зберігати старих. CRM-системи стали першим видом інформаційних систем, які сфокусували увагу керівників не на бек-офісі, як в системах ERP, і не на виробничих процесах, як в системах MRP, MRP II, а на фронт-офісі – в маркетингу, продажах, сервісі та обслуговуванні.

На підставі отриманих результатів дослідження був розроблений модуль управління відносинами зі споживачем, для чого був підготовлений технічний опис банківської CRM-платформи на базі Shugar CRM, побудовано схему та ролі управління правами доступу в автоматизованій CRM-системі, а також сформульовано основні вимоги щодо побудови системи інформаційної безпеки, як важливої складової будь-якої автоматизованої системи управління відносинами зі споживачем.

Програмний модуль системи управління відносинами зі споживачем дозволяє автоматизувати бізнес-процеси, пов'язані з маркетингом, продажами та обслуговуванням. Як результат – розробка персоніфікованої пропозиції конкретному клієнту, яка пропонується йому в певний, сприятливий для угоди, час та передається йому найзручнішим для нього каналом комунікації. CRM-система забезпечує координацію дій різних підрозділів на основі загальної інформаційної платформи для взаємодії з клієнтами, а вбудовані механізми захисту забезпечуватимуть необхідний рівень безпеки інформації, що зберігається в системі, відповідно до вимог сучасного бізнесу та національного законодавства.

Науковий керівник — к.т.н. Василь Бриль

Особенности защиты программного обеспечения специализированных авиационных тренажеров

УДК 629.735.072.8.08:004(045)
Владимир Моржов, Юрий Ермачков
Національний авіаційний університет, Україна author1morzhov@ua.fm

Широкое внедрение цифровой вычислительной техники в имитаторы бортовых систем воздушных судов (ВС) современных авиационных тренажеров (АТ) различного типа создало определенные трудности по защите от несанкционированного копирования моделей АТ.

Ранее разработанные методы защиты информации в аналоговых АТ не могут быть использованы в современных цифровых АТ.

К числу основных факторов, обуславливающих необходимость разработки эффективных методов по защите аппаратно-программных средств АТ, относятся: обеспечение недоступности информации о характеристиках ВС и его систем, которая является собственностью организаций-разработчиков и не может передаваться никому без их ведома; защита авторских прав разработчиков авиационной техники, которая моделируется в имитаторах АТ и разработчиков аппаратных и программных средств тренажерной техники.

Вся информация о технических характеристиках и структуре построения бортовых систем, а также об аэродинамических и высотно-скоростных характеристиках моделируемых ВС (особенно военных и специального назначения) хранится на жестких магнитных дисках. Эти устройства позволяют достаточно просто осуществлять копирование информационных массивов, находящихся на них.

Все это заставляет разрабатывать специальные проектные решения АТ, которые бы обеспечили невозможность несанкционированного доступа и копирования ПО АТ.

В связи с этим, решение этой задачи следует искать при проектировании АТ, в частности при разработке ПО имитаторов АТ.

АТ различного типа имеют свои как аппаратные, так и программные особенности, которые должны учитываться при разработке средств защиты от несанкционированного копирования информации.

Основной конструктивной особенностью является модульный принцип построения программного обеспечения, каждый модуль которого реализует математическую модель соответствующей авиационной системы.

Вся совокупность модулей имитаторов тренажера представлена в главном меню тренажера.

В этой связи, для такой организации ПО целесообразно осуществлять защиту индивидуально по каждому модулю, т.е. доступ к конкретному имитатору тренажера будет осуществляться только после подтверждения авторизации.

Представляет интерес использовать устройство USB в качестве мини HASP аппаратного ключа (Hardware Against Software Piracy).

Целесообразность такого использования объясняется следующими факторами: 1) незначительная цена таких аппаратных ключей; 2) длительный срок использования ПО АТ; 3) индивидуальный алгоритм защиты от несанкционированного копирования информации.

В общем случае порядок организации защиты ПО от несанкционированного копирования необходимо осуществлять в следующей последовательности: 1) выбрать тип USB-устройства, которое будет использовано в качестве HASP аппаратного ключа; 2) определить серийные номера PID и VID USB-устройства; 3) определить точки входа в ПО тренажера через файл USB-ключа; 4) написать программу шифрования с использованием

криптографического алгоритма; 5) обеспечить автономность работы АТ (ЦВМ не должна быть подключена к любой компьютерной сети).

Таким образом, особенности построения ПО специализированных АТ и их аппаратных средств показывают, что эффективная защита информации может быть реализована на основе USB-устройств. Файл-ключ, записанный на указанном устройстве, открывает доступ к определенной программе цифровой модели имитатора АТ.

Все эти требования должны быть изложены в тактико-техническом задании на специализированный тренажер конкретного типа ВС.