У статті розглянуто питання побудови політики безпеки для технологій, які використовують віртуалізацію, приведені принципи, які використовуються для побудови політики безпеки, а також наводяться приклади напрямів захисту інформації, які слід враховувати при побудові політики безпеки.
Ключові слова: політика безпеки, інформаційна безпека, віртуальне середовище.

В статье рассматривается вопрос построения политики безопасности для технологий, которые используют виртуализацию. Определены принципы, которые используются для построения политики безопасности, а также приводятся примеры направлений защиты информации, учитываемые при построении политики безопасности.
Ключевые слова: политика безопасности, информационная безопасность, виртуальная среда.

In this article the question of construction of policy of safety is considered for technologies which use a virtualization, principles which are used for the construction of policy of safety are resulted, and also examples of directions of defence information are made, which are necessary to take into account at the construction of policy of safety.
Keywords: security policy, information security, virtual environment.

Поступила 27.04.2010

УДК 681.3.96

к.т.н. Волощенко А.С.
військова частина Е-6133

КОНЦЕПТУАЛЬНІ ПІДХОДИ ВПРОВАДЖЕННЯ НОВІТНІХ ТЕХНОЛОГІЙ ДО ПОБУДОВИ КОМПЛЕКСІВ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

Проблема забезпечення ефективного технічного захисту інформації набуває все більшої актуальності, що обумовлено багатьма причинами, пов'язаними як із загальним технічним прогресом у всьому світі, так і з внутрішніми політичними, економічними та соціальними факторами. Присутня на теперішній час підвищена вразливість інформації, що обробляється, передається та зберігається із застосуванням засобів обчислювальної техніки, зв'язку, запису, розмножувальної техніки та інших технічних засобів і систем, якими в теперішній час широко устатковуються будь-які державні та комерційні структури, є наслідком стрімкого розвитку як самих перелічених технічних засобів та систем, так і методів та засобів перехоплення інформації.

Розвиток ринкових відносин в нашій державі загострив проблему безпеки інформації, при цьому стрімкого розвитку набули два процеси:

- перший, з добутку інформації або завдання їй деструктивної шкоди;
- другий, із захисту інформаційних ресурсів.

За умов політики відкритості та свободи преси, особливо важливим стає забезпечення ефективного захисту інформації. Ця проблема однаково актуальна для інформаційних систем, систем зв'язку та управління, що належать підприємствам різної форми власності, взагалі там, де циркулюють великі об'єми інформації різного рівня конфіденційності.

Для запобігання витоку інформації технічними каналами є необхідними спеціальні заходи, методи та засоби захисту.

Слід відмітити, що активний метод захисту (зашумлення) розвивався інтенсивніше та швидше впроваджувався, оскільки не потребував серйозних фінансових витрат при виробництві. Така ситуація зберігалася до початку 90-х років минулого століття. Процес, так званої, перехідної економіки згенерував створення структур недержавної власності, що займаються проблемами безпеки інформації, до яких увійшли досвідчені фахівці з державних підприємств та організацій. Доступнішими стали новітні технології і публікації з питань інформаційної безпеки. Зазначені фактори стимулювали прискорення розвитку низки методів, способів та засобів захисту інформації.

Розширення спектру вимог, які стало необхідно враховувати при виготовленні технічного засобу обробки інформації в спеціальному виконанні, викликало зміни в концепції його комплексного захисту. Наприклад, при застосуванні активного методу захисту необхідно розуміти сутність його негативного впливу для вирішення задачі забезпечення біологічного захисту оператора від створюваного потужного шумового поля.

В зв'язку з цим все більша увага стала приділятися програмно-апаратним засобам та пасивному методу технічного захисту, зокрема електромагнітному екрануванню.

Під останнім розуміється створення захисних екранів з високою ефективністю дії в широкому частотному діапазоні. Основною технічною характеристикою захищеності в цьому аспекті є величина ефективності екранування матеріалу екрана. Збільшення цієї величини дозволяє зменшити радіус контрольованої зони, що ускладнює задачу з перехоплення інформації каналами побічних електромагнітних випромінювань і наведень.

Актуальності набуває розробка принципів побудови широкосмугових захисних електромагнітних екранів з заданими властивостями, розробка рекомендацій по керованій зміні їх електромагнітними параметрами в заданому напрямку.

З боку запобігання витоку інформації технічними каналами, при створенні захищених корпусів засобів електронно-обчислювальної техніки вбачається перспективним застосування спеціальних покриттів з нанокристалічною структурою (рис.1).

Наноструктурний стан є "каталізатором" фізичних властивостей металевих матеріалів. В такому стані металеві матеріали проявляють набагато вищі електромагнітні та міцнісні характеристики, поясненням чого є ступінь гетерогенності та композиційний ближній порядок атомної структури.

Практична і відносно недорога технологія нанесення наноструктурних покриттів методами газотермічного напилювання (ГТН) дозволяє виготовляти окремі екрановані панелі. У цьому аспекті ГТН має широкі можливості надання поверхням виробів спеціальних електромагнітних властивостей. Багатокомпонентним нанокристалічним сплавам на основі металів групи заліза, отриманим гартуванням з розплаву або методами ГТН властива градієнтність електромагнітних і як наслідок екрануючих властивостей. Шляхом створення градієнтних нанокристалічних феромагнетиків з певним розподілом за розмірами нанофаз та відповідним розміщенням їх у аморфній матриці можливо цілеспрямовано управляти величиною амплітудного послаблення та максимально розширити частотний діапазон ефективності дії захисних екранів [1].

Принцип екрануючої дії захисних електромагнітних екранів на основі наноструктурних феромагнетиків полягає в наступному. Під впливом зовнішнього магнітного поля H вектор намагніченості в доменах повертається на деякий кут у напрямку поля, що призводить до зміни польової залежності намагніченості $J = f(H)$. Послаблення електромагнітної енергії відбувається через зростання енергії матеріалу у зовнішньому магнітному полі, витрат на рух доменних границь та зміну їх структури.

Багатокомпонентні швидкозагартовані сплави на основі металів групи заліза, отримані методами гартування з розплаву або методами ГТН є мікрогетерогенними і характеризуються наявністю структурних та концентраційних неоднорідностей нанорозмірних масштабів. Величину таких неоднорідностей та їх просторовий розподіл можна змінювати як шляхом легування сплавів, так і зміною технологічних умов їх формування. Наявність кластерів певних розмірів у матриці аморфних феромагнетиків дозволяє в широких межах змінювати їх електромагнітні та екрануючі властивості.

На теперішній час забезпечення цілісності та доступності інформації зумовлює появу додаткових вимог щодо інформаційної безпеки в цілому.

Зокрема, однією із загроз інформації в інформаційно-телекомунікаційних системах (ІТС), визначеною у більшості моделей загроз, є апаратні збої, причиною яких є вихід з ладу апаратури та пошкодження носіїв інформації.

Носії інформації є одним з найважливіших вузлів в електронно-обчислювальних машинах та основною базою зберігання даних. Прогрес в техніці призводить до постійного зростання ємності накопичувачів інформації за рахунок збільшення щільності запису на поверхні диску. До речі, за останнє десятиліття відбулося збільшення ємності накопичувачів на жорстких дисках приблизно в 1000 разів [2].

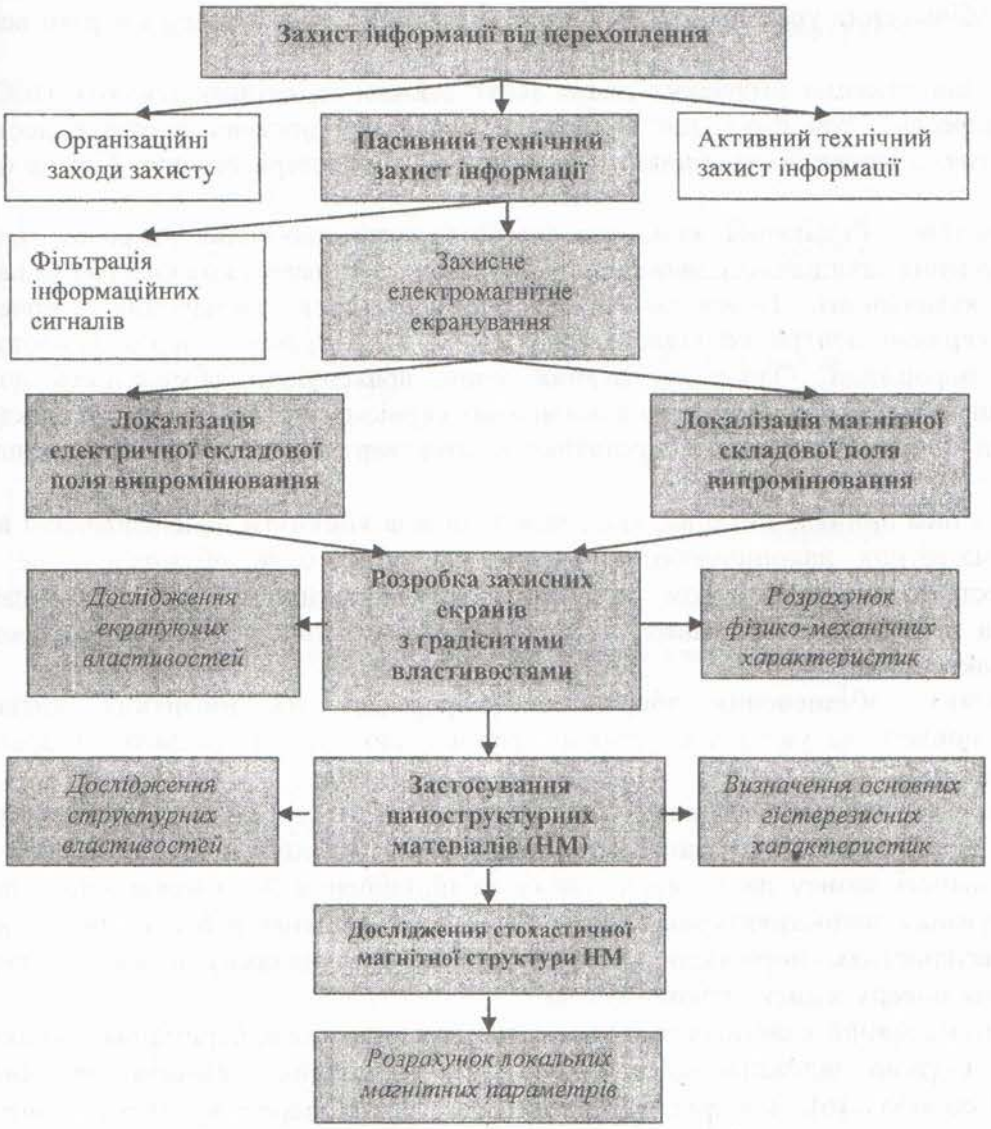

Рис.1. Концептуальна схема впровадження нанотехнологій при організації пасивного технічного захисту інформації

В основі функціонування вінчестера покладено принцип магнітного запису/зчитування сигналів на диск-накопичувач, покритий магніточуттєвим робочим шаром. Кожна сторона диску, покрита робочим шаром є робочою поверхнею. При зчитуванні інформації голівки блоку позиціонеру знаходяться над диском-накопичувачем лише на відстані 0,05...0,12 мкм, доріжка рухається під магнітною голівкою зі швидкістю 90...125 км/год [3]. Очевидно, що зовсім несуттєвий удар призведе до величезних руйнівних наслідків (в сучасних накопичувачах поверхнева щільність запису складає 65-70 Гбіт/кв.дюйм). Слід зазначити, що при ударі магнітної голівки о поверхню диска вилітає мікроскопічний осколок, який вдаряючись об обертаючийся зі швидкістю ~10^4 обертів на хвилину диск, вибиває наступний

осколок. Такий процес має лавинний характер і вихід накопичувача з ладу неминучий. Навіть у випадку, коли пошкодження не велике, вибиті при ударі частки магнітного покриття ще протягом тривалого часу будуть літати всередині корпусу диска, створюючи небезпеку нової аварії, причому більша їх частина взагалі не лишає диск, лишаючись "примагніченою" до його поверхні, приводячи до подальшого її руйнування. Таким чином, підвищення щільності запису у сучасних накопичувачах, збільшення швидкості обертання пластин призводять до збільшення уразливості дисків від механічних пошкоджень і втрати великих об'ємів даних.

Проблема відновлення втрачених даних існує стільки ж, скільки існують ПЕОМ. Її значущість підкреслює той факт, що надійність сучасних жорстких дисків є достатньо низькою. Практично жоден з виробників не дає на свої вінчестери гарантії більше одного року.

Через постійне збільшення кількості засобів електронно-обчислювальної техніки, питання забезпечення захищеності даних в інформаційних системах з кожним роком набуває все більшої актуальності. Внаслідок цього спостерігається збільшення звернень у спеціалізовані сервісні центри по відновленню інформації, втраченої через пошкодження накопичувачів інформації. Однак, за певних умов, враховуючи обмеженість доступу оброблюваної інформації, звернутися до комерційних сервіс-центрів не завжди є можливим. Крім того, слід приймати до уваги, достатньо високу вартість послуги по відновленню інформації.

В зв'язку з цим виникає питання, яким чином можна уникнути непередбаченої втрати інформації з магнітних накопичувачів, до речі яка може бути обумовлена не лише навмисним деструктивним впливом потужних електромагнітних імпульсів, свідомо направлених на руйнування баз даних, але і механічними ушкодженнями, викликаними випадковими факторами.

Проблематика забезпечення збереження інформації на магнітних дисках – накопичувачах привертала увагу дослідників і раніше, що сприяло розвитку теоретичної думки в даній галузі [2, 4, 5].

Впровадження сучасних наукових технологій, дозволяє комплексно вирішувати питання щодо збереженості інформації від деструктивних впливів в ІТС в частині щодо збільшення щільності запису на поверхні диску та підвищення його механічної міцності шляхом застосування наноструктурних матеріалів (яким властиві набагато більш високі міцнісні характеристики порівняно з кристалічними матеріалами) в якості основної складової робочої поверхні диску-накопичувача.

Магнітні та механічні властивості наноструктурних матеріалів, отриманих швидкісним загартуванням, суттєво залежать від технології їх отримання, режимів термічної та термомагнітної обробок [6]. Зокрема, залежний від ступеня перегріву структурний стан матеріалу визначає рівень магнітної анізотропії та величину коерцитивної сили, що є основною магнітною характеристикою робочої поверхні накопичувача інформації.

Наноструктурні покриття характеризуються високими значеннями мікротвердості, рівень якої в першу чергу визначається системою легування.

Проведений аналіз вказує на перспективи використання наноструктурних матеріалів в якості покриттів робочих поверхонь накопичувачів інформації, підбір оптимальних умов отримання таких покриттів дозволяє досягти великих значень мікротвердості, тим самим роблячи накопичувач більш захищеним від механічних ушкоджень [5]. Однак однозначно стверджувати про підвищення міцнісних властивостей робочих поверхонь можливо лише після проведення практичних і теоретичних досліджень адгезії та зносостійкості, а також впливу цих характеристик на коерцитивну силу (рис.2).

Актуальність таких досліджень визначається як потребою залучення прогресивних наукоємних технологій в створенні автоматизованих комплексів прийому, збереження та

захисту інформації в комп'ютерних системах, так і інтересом фундаментальної науки до технологій нового покоління, якими є отримання наноструктур із заданими фізичними властивостями. Впровадження у галузь комплексного захисту інформації наноструктур вимагає як оптимізації технології їх отримання, так і комплексного дослідження їх структури та фізичних властивостей сучасними методами.

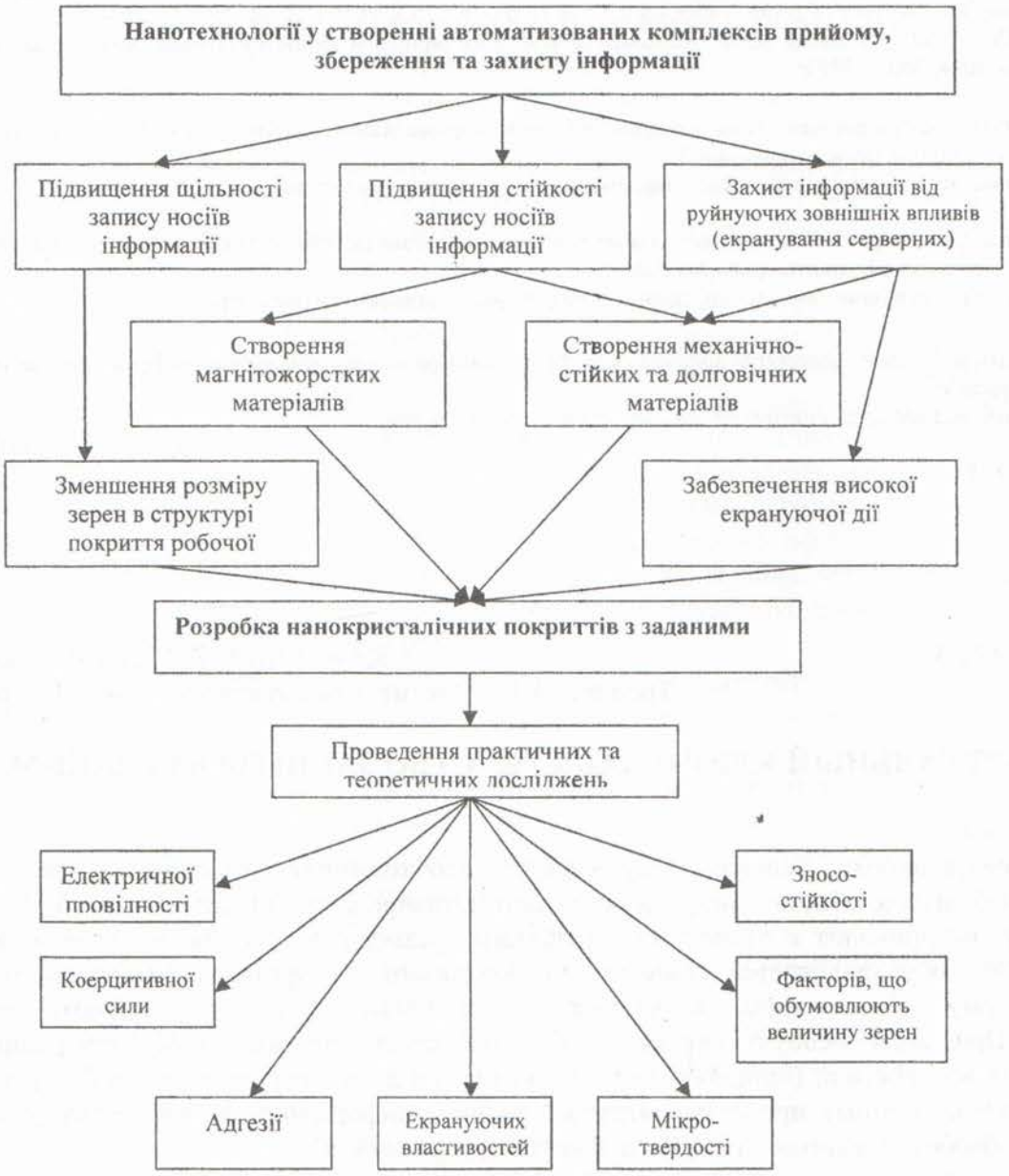

Рис.2. Концептуальна схема впровадження нанотехнологій при створенні автоматизованих комплексів в захищеному варіанті

Важливість досліджень обумовлюється тим, що до теперішнього часу не розроблено наукові принципи забезпечення збереженості інформації при вирішенні проблеми локалізації деструктивних впливів у комп'ютерних системах, одним з напрямків вирішення якої є застосування наноструктурних систем у складі накопичувачів інформації та захисних екранів - локалізаторів електромагнітних полів.

Список літератури

1. *Сенюк И.А.* "Этот сложный жесткий диск".: - Науково-технічний журнал "Камуфляж", 2004 р. №5(19).
2. *Коженевский С.Р.* Безопасность хранения информации на жестких дисках.: - Зб. наук. праць НАН України, 2003 р. №4. – С. 67-84.
3. *Волощенко А.С., Остапенко Г.П.* Забезпечення збереженості даних в сучасних автоматизованих системах шляхом покращення фізичних властивостей накопичувачів інформації// Зб. наук. праць "Спеціальні телекомунікаційні системи та захист інформації".- № 1(10).– К.: ДССЗЗІ України.- 2005.– С.56-61.
4. *Шпак А.П., Куницкий Ю.А., Карбовский В.Л.* Кластерные и наноструктурные материалы. т.1.- К.: Академпериодика, 2001.- 588 с.

В статті розглядаються концептуальні підходи впровадження новітніх технологій до побудови комплексів технічного захисту інформації.
Ключові слова: новітні технології, захист інформації, електромагнітний екран.

В статье рассматриваются концептуальные подходы внедрения новейших технологий к построению комплексов технической защиты информации.
Ключевые слова: новейшие технологии, защита информации, электромагнитный экран.

The article discusses conceptual approaches to the introduction of new technologies to build complex technical information security.
Keywords: new technologies, information security, electromagnetic screen.

Надійшла 13.04.2010

УДК 004.621.3

Климентов В.В. (ООО «Парисет»),
Трощило А.С. (Институт радиоэлектроники АН Украины)

«ВИРТУАЛЬНЫЙ КЛЮЧ» КАК СРЕДСТВО ЗАЩИТЫ БАЗ ДАННЫХ

Введение

В современных условиях ссуществует необходимость быстрой и корректной обработки больших объемов информации автоматизированными системами (АС), что, в свою очередь, приводит к появлению проблемы чрезмерных сетевых нагрузок и защиты данных. Это обусловливается общими требованиями к организации, аппаратному и программному обеспечению, в частности, к системам управления базами данных (СУБД). При этом особую актуальность приобретает защищенность информации от негативных воздействий (хищения, видоизменения и т.д.) непосредственно в базах данных (БД) и СУБД. Поэтому проблема надежной защиты информации в автоматизированных системах обработки данных (АСОД) становится приоритетной.

Одним из вариантов решения данной проблемы может рассматриваться защита АСОД с помощью криптографических методов и средств. Анализ работ [1,2], посвященных оценке качества программных средств АСОД, позволяет применить практически весь набор характеристик и атрибутов стандарта ISO 9126 «Качество программных средств» для использования в составе требований к СУБД. По сути, они сводятся к возможности контроля изменений в состоянии базы данных и являются главным свойством всех мероприятий, направленных на соответствие требованиям.В исследованиях [3,4], посвященных анализу методов и средств защиты информации в АСОД, сделаны попытки измерить и описать качество защищенности информации обобщенно, трудоемкостью и временем, необходимыми для преодоления злоумышленниками системы защиты. При этом косвенным