MATERIÁLY
XIV MEZINÁRODNÍ VĚDECKO - PRAKTICKÁ KONFERENCE

AKTUÁLNÍ VYMOŽENOSTI VĚDY - 2018

22 - 30 června 2018 r.

Volume 9

Stavebnictví a architektura
Matematika
Moderních informačních technologií
Fyzika

Praha
Publishing House «Education and Science»
2018

Vydáno Publishing House «Education and Science»,
Frýdlanská 15/1314, Praha 8
Spolu s DSP SHID, Berdianskaja 61 B, Dnepropetrovsk

Materiály XIV Mezinárodní vědecko - praktická konference «Aktuální vymoženosti vědy -2018», Volume 9 : Praha. Publishing House «Education and Science» -68 s.

Šéfredaktor: Prof. JUDr Zdenák Černák

Náměstek hlavního redaktora: Mgr. Alena Pelicánová

Zodpovědný za vydání: Mgr. Jana Štefko

Manažer: Mgr. Helena Žákovská

Technický pracovník: Bc. Kateřina Zahradníková

Pro studentů, aspirantů a vždeckách pracovníků

Cena 50 kč

ISBN 978-966-8736-05-6

MODERNÍCH INFORMAČNÍCH TECHNOLOGIÍ

Computer engineering

Нукусова Б.К.
Қ.Жұбанов атындағы орта мектеп
Ақтөбе облысы, Мұғалжар ауданы, Жұрын ауылы, Қазақстан

ИНФОРМАТИКА ПӘНІ БОЙЫНША КРИТЕРИАЛДЫҚ БАҒАЛАУДЫ ЖОСПАРЛАУ ЖӘНЕ ҰЙЫМДАСТЫРУ

Қазіргі білім беру жүйесінің ерекшелігі оның негізгі тауары- құзіреттілік, яғни білім алушының қандай да бір іс-әрекетке құзіреттілігін дамыту, арттыру, қалыптастыру. Біз оқушының білімін, біліктілігін, дағдысын бағалаудан оның құзіреттілік қасиетінің қалыптасуын бағалауымыз керек.

Бағалау білім беру процесінің қажетті құрамдас бөлігі болып табылады, яғни оқытудың ағымдағы және соңғы сатыларында оқушылардың жетістіктері туралы ақпаратты жинау және талдау. Бағалаудың мақсаты, пәні, нысаны, қағидалары, әдістері, формалары мен құралдары білім беру процесінің барлық субъектілері, яғни мектеп әкімшілігі, мұғалімдер, ата-аналар және оқушылардың өзіне түсінікті болуы керек. Бағалау жүйесі - бұл білім беру сапасын әлемдік стандарттарға сәйкестігін анықтауға, білім беру саласындағы ағымдағы міндеттерге сәйкес келмеген жағдайда білім беру стратегиясына және тактикасына қатысты түбегейлі шешімдер қабылдауға, білім берудің мазмұнын жетілдіруге мүмкіндік беретін оқудың мәселелерін диагностикалаудың негізгі құралы болып табылады.

Бағалау - алынған нәтижелер мен жоспарланған мақсаттар арасындағы қатынас процесі. Оқытудың қаншалықты табысты, ойдағыдай өтетіні, сондай-ақ, білім алушылардың қандай қиындықтарды басынан өткізетіндігі туралы ақпаратты мектептің тиімді бағалау жүйесі көрсететіндігін жоғарыда атап өткен болатынбыз. Сондықтан да қазіргі таңда жаңартылған білім беру мазмұнын енгізу кезінде критериалды бағалау жүйесі қолданылады.

Критериалды бағалау білім алушылардың оқу жетістіктерін салыстыру процесіне негізделген, оқушылардың оқу-танымдық құзыреттілігін қалыптастыруға ықпал ететін білімнің мақсаттары мен мазмұнына сәйкес процестің барлық қатысушылары үшін белгілі бір ұжымдық әзірленген критерийлермен салыстыру негізінде жүзеге асырылатын бағалау жүйесі. Бұл бағалау рәсімдерінің сапалылығын, олардың халықаралық стандарттарға сәйкестігін және әр білім алушының оқудағы қажеттілігін қамтамасыз етуге мүмкіндік береді. Қазақстан үшін ұсынылып отырған жаңа критериалды бағалау жүйесі білім алушының дамуын, оның қызығушылығын және оқуға деген ынтасын арттыруға бағытталады. Егер әр білім алушыға және оның ата-анасына түсінікті болатындай нақты әрі өлшемді бағалау критерийлері белгіленетін болса, бұған жетуге әбден болады. Анық құрастырылған бағалау критерийлерінің көмегімен мұғалім де, білім алушы да:

- Білім алушы оқытудың қай сатысында?

- Олар білім алуда неге талпынады?

- Бұған жетуге көмектесу үшін не істеу керек? екенін түсінеді.

Критериалды бағалау –оқушылардың білім жетістіктерін ұжыммен келісілген, оқу үрдісіне қатысушыларға алдын-ала белгілі, оқушылардың негізгі құзыреттіліктерінің қалыптасуына жағдай жасайтын, білім берудің мақсаты мен мазмұнына сәйкес нақты анықталған критерийлер бойынша салыстыруға негізделген үрдіс.

Критериалды бағалау жүйесінің мақсаты бағалау критерийлерінің негізінде білім алушылардың оқу жетістіктері туралы шынайы ақпарат алу және оқу үдерісін жетілдіре түсу үшін оны барлық қатысушыларға ұсыну.

Критериалды бағалау жүйесінің міндеттері:

1. Оқу үдерісінде бағалаудың қызметі мен мүмкіндіктері аясын кеңейту;

2. Жүйелі кері байланыс орнату арқылы білім алушылардың өзін-өзі үнемі жетілдіріп отыруына жағдай жасау;

3. Бірыңғай стандарттарды, сапалы бағалау құралдарын, механизмдерін қалыптастыруға көмектесу;

4. Қолжетімді, нақты, үздіксіз:

– білім алушыларға олардың оқу сапасы туралы;

– мұғалімдерге білім алушылардың ілгерілеуі туралы;

– ата-аналарға оқу нәтижелерінің деңгейлері туралы;

– басқару органдарына ұсынылған білім беру қызметінің сапасы туралы ақпараттар ұсыну.

Информатика» пәні бойынша оқушылардың білімдік жетістіктерін бағалаудың жалпы критерийлері

Критерийлер		Максималды деңгей
A	Білу және түсіну	5
B	Зерттеу	4
C	Жоспарлау	4
D	Жоба құру	5
E	Дизайн	3
F	Коммуникация	3
G	Рефлексия	3
Барлығы		27

Бағалау жүйесінің негізгі мақсаты- білім сапасын арттыру болып табылады. Ал қазіргі заманғы білім сапасы дегеніміз ол білім алушының келешектегі өзінің әртүрлі жеке мәселелерін шешуге керекті, қажетті құзіреттіліктерін қалыптастыратын білім беру нәтижесі.

Әдебиеттер:

1. Международные исследования PISA:Национальный отчет по итогам международного исследования PISA-2009 в Казахстане/ 2010 //Электронный ресурс. – Режим доступа: naric.kz›index-49.php.htm.
2. Государственная программа развития образования Республики Казахстан на 2011-2020 годы. Указ Президента Республики Казахстан от 7 декабря 2010 года № 1118.
3. . Красноборова А. А. Критериальное оценивание как технология формирования учебно-познавательной компетентности учащихся // Автореф. … канд. дисс Нижний Новгород – 2010. – 140 с.

Стовбчатий М. М.
Вінницький національний технічний університет,Україна

ВСТАНОВЛЕННЯ АВТОРСТВА ТЕКСТУ ЗА ДОПОМОГОЮ ДЕРЕВ ЗАЛЕЖНОСТЕЙ

Атрибуція тексту - дослідження тексту з метою встановлення авторства або отримання будь-яких відомостей про автора, завдання атрибуції можна розділити на ідентифікаційні та діагностичні.

Ідентифікаційні завдання дозволяють здійснити перевірку авторства:

підтвердити авторство певної особи;

виключити авторство певної особи;

перевірити той факт, що автором всього тексту була одна і та ж особа;

перевірити той факт, що той хто написав цей текст є при цьому його справжнім автором.

Ідентифікаційні завдання вирішуються з припущення, що автор тексту відомий. Діагностичні завдання дозволяють визначити як особистісні характеристики автора (освітній рівень, рідна мова, знання іноземних мов, походження, місце постійного проживання тощо), так і факт свідомого спотворення письмової мови. Діагностичні завдання вирішуються з припущення, що автор тексту невідомий.

Методи атрибуції дозволяють досліджувати текст на п'яти рівнях: пунктуаційному, орфографічному, синтаксичному, лексико-фразеологічному, стилістичному.

Пунктуаційний рівень допомагає виявити особливості вживання автором знаків пунктуації, характерні помилки.

Орфографічний рівень виявляє характерні помилки в написанні слів.

Синтаксичний рівень дозволяє визначити особливості побудови речень, перевагу тих чи інших мовних конструкцій, вживання часів, активного або пасивного стану, порядок слів, характерні синтаксичні помилки.

Лексико-фразеологічний рівень визначає словниковий запас автора, особливості використання слів і виразів, схильність до вживання рідкісних і іноземних слів, діалектизмів, архаїзмів, неологізмів, професіоналізмів, арготизмів, навички вживанням фразеологізмів, прислів'їв, приказок, «крилатих виразів» і т. і.

Стилістичний рівень дозволяє визначити жанр, загальну структуру тексту, для літературних творів – сюжет, характерні зображальні засоби (метафора, іронія, алегорія, гіпербола, порівняння), стилістичні фігури (градація, антитеза, риторичне питання тощо), інші характерні мовні прийоми.

Під «авторським стилем» зазвичай розуміються останні три рівня. Аналіз саме синтаксичного, лексико-фразеологічного та стилістичного рівнів представляє найбільший інтерес і найбільшу складність [1].

До проблем, що ускладнює дослідження в області атрибуції текстів, відноситься також проблема складання вибірки еталонних текстів. Бажано, щоб твори були підібрані таким чином: тексти різних письменників в максимальному ступені відмінності один від одного, а тексти одного письменника були максимально близькі. Але існує не-мало випадків, коли відомий письменник в якийсь період своєї творчості міняв стиль викладу, або твори були написані в співавторстві. Ці факти створюють додаткові складності при вирішенні завдання встановлення авторства.

Побудова ДЗ відповідає таким умовам:

1. Дерево повинно мати тільки одну вершину (рис. 1.1).

2. Кожній словоформі у реченні відповідає один вузол у ДЗ.

3. Ребро відповідає зв'язкові між двома словоформами. Напрям ребра – від словоформи, яка підпорядковує ("хазяїн"), до словоформи, яка підпорядковується ("слуга").

4. Усі ребра є орієнтованими, тобто напрям ребер дерева наперед визначений: від вершини до вузлів, які розташовані в дереві рівнем нижче.

5. В один вузол може входити не більше одного ребра.

6.Дерево має бути зв'язним, тобто у дереві не може бути вузлів, не пов'язаних з іншими вузлами дерева.

7. У дереві не може бути циклів, тобто ребро не може входити у вузол, із якого воно виходить.

8. Вершиною дерева можуть виступати присудки простого двоскладного речення, головний член односкладного речення, присудок головної частини складнопідрядного речення.

Така інтерпретація синтаксичної структури речення ґрунтується на лінгвістичній моделі "Смисл ⇔ Текст" І.О. Мельчука [Мельчук 1974][2].

Рис. 1.1 - Дерево залежностей для речення з аналітичною лексемою, сурядністю та еліпсисом*.

В основі моделі дерева лежить уявлення про побудову речення як про послідовне попарне синтагматичне зчеплення складових від мінімальних – окремих слів, до максимальної - речення, складовими якого, в загальному випадку, є група підмета і група присудка.

Подання синтаксичної структури в термінах дерева складових добре узгоджується з традиційним «розбором» речення, при якому підмет, присудок та інші елементи описуються категоріальним характеристиками – іменами частин мови або груп.

Граф – це засіб представлення змісту у вигляді семантичної зв'язку, це перекодування, структуризація знання. В основі перекодування лежить угруповання, смислова організація матеріалу. Граф виступає як засіб, з одного боку, фіксації структурно смислових компонентів тексту, а з іншого боку, контролю мовного продукту, тобто як механізм звірення і оцінки відповідності значення і форми деякої мовної структури до ідеалу [2].

У загальному вигляді методика побудови графа денотативної структури полягає в тому, що з тексту виділяються об'єкти (денотат), про які йдеться в тексті, і та інформація, яка повідомляється про них. Ця інформація виражається у вигляді інших об'єктів, пов'язаних з першими певними відносинами. Імена виділених об'єктів фіксуються у вигляді вершин графа, які розташовуються в певній послідовності. Ця послідовність визначається поданням про перехід від

теми до підтемах, від загального до конкретного, від цілого до частини. При побудові такого графа аналіз тексту проводиться глобально, тобто окремі пропозиції не обов'язково виступають в якості одиниць аналізу. Тому розташування вершин графа може не відповідати порядку проходження об'єктів в тексті, а відображати скоріше їх об'єктивне, предметне співвідношення.

Всі операції, пов'язані з побудовою графа, носять змістовний характер. Побудова такого графа є своєрідний спосіб матеріалізації результату розуміння. Сама графічна форма робить структуру відношень між елементами різних рівнів тексту наочною і доступною для огляду, сприяє більш повному і глибокому розумінню змісту тексту.

Як показала практика, подібна методика формалізації тексту дозволяє побачити скелет автора, тобто його стиль написання творів, прискорити процес засвоєння, осмислення і репродукції тексту, допомагає учням, використовуючи різні мовні моделі, складати свої варіанти монологічних висловлювань по темі, досить швидко виводить їх у вільну комунікацію, сприяє формуванню семіотичної компетенції. Подібна кодова модель комунікації дозволяє підтримувати основоположні здатності природного інтелекту – здатність до абстрагування та згортки знання [3].

ЛІТЕРАТУРА:

1. Романов А. С. Методика и программный комплекс для идентификации автора неизвестного текста: Автореф. дис. ... канд. техн. наук. Томск, 2010. 26 с .
2. Севбо И. П. Графическое представление синтаксических структур и стилистическая диагностика / Ирина Платоновна Севбо. – Місто: Киев: Наукова думка, 1981. – 132 с.
3. Бісікало О. В. Метод визначення ключових слів англомовного тексту на основі DKPRO CORE / Бісікало О.В, Яхимович О.В. – "Технологічний аудит та резерви виробництва". – Том 1, № 2(21). – 2015. – С. 12 – 14.

Мадеш Ж.М.
Магистрант Казахской академий труда и социальных отношений, Казахстан, Алматы

РАЗРАБОТКА МЕТОДИКИ И АЛГОРИТМА ПОИСКА И ЛОКАЛИЗАЦИИ НЕИСПРАВНОСТЕЙ В СЕТЯХ ТИПА ATM

Поддержка объединенной сети связана с ежедневным решением ряда проблем с устранением тех или иных неполадок. Большая часть нареканий на работу объединенных сетей в наши дни так или иначе связаны с их производительностью: медленная работа сети, зависание сетевого файл- сервера, прерывания обслуживания во время выполнения определенных операций файл-сервера и т. п. Очевидно, что в основном эти проблемы относят к сбоям сетевой связи, вызванным неправильной конфигурацией и компоновкой аппаратных и программных средств.

Бывает так, что изменение простого параметра конфигурации или небольшая модификация компоновки технических или программных средств, - вот и все, что требуется для достижения оптимального функционирования системы. Также очень часто для устранения неполадки в сети требуется хорошая интуиция аналитика или программиста.

Данный дипломный проект освобождает аналитика от непредсказуемых предугадываний симптомов неисправностей и их локализации. Для работы с данной программой специалисту потребуются лишь хорошее знание и опыт работы с сетью, так как в программе детально разработана схема поиска и локализации всех возможных неисправностей в локальной сети типа ATM.

Структура сети ATM Базовые принципы, лежащие в основе технологии ATM, могут быть выражены в трех утверждениях:

сети ATM - это сети с трансляцией ячеек (cell-relay);

сети ATM - это сети с установлением соединения (connection-oriented);

сети ATM - это коммутируемые сети.

Подход, реализованный в технологии ATM, состоит в представлении потока данных от каждого канала любой природы - компьютерного, телефонного или видеоканала пакетами фиксированной и очень маленькой длины - 53 байта вместе с небольшим заголовком в 5 байт. Пакеты ATM называются ячейками - cell. Небольшая длина пакетов позволяет сократить время на их передачу и тем самым обеспечить небольшие задержки при передаче пакетов, требующих постоянного темпа передачи, характерного для мультимедийной информации. При приоритетном обслуживании мультимедийного трафика коммутаторами сети, его пакеты будут вынуждены даже при дисциплине относительных приоритетов ожидать в худшем случае в течение небольшого и фиксированного времени - времени передачи пакета из 53 байт, что при скорости в 155 Мб/с составит менее 3 мкс. Для того, чтобы пакеты содержали адрес узла назначения и в то же время процент служебной информации не был большим по сравнению с размером поля данных пакета, в технологии ATM применен стандартный для глобальных вычислительных сетей прием - эти сети всегда работают по протоколу с установлением соединения и, адреса конечных узлов используются только на этапе установления соединения. При установлении соединения ему присваивается текущий номер соединения и в дальнейших передачах пакетов в рамках этого соединения (то есть до момента разрыва связи) в служебных полях пакета используется не адрес узла назначения, а номер соединения, который намного короче.

В пакете имеется небольшой заголовок в 5 байт, из которых 3 байта отводятся под номер виртуального соединения, уникального в пределах всей сети ATM, а остальные 48 байт могут содержать 6 замеров оцифрованного голоса или 6 байт данных вычислительной сети. Небольшие пакеты фиксированной длины позволяют гарантировать небольшие задержки при передаче синхронного трафика. Ясно, что при отказе от жестко фиксированных канальных интервалов для каждого канала, идеальной синхронности добиться будет невозможно.

Однако, если пакеты разных видов трафика будут обслуживаться с разными приоритетами, то максимальное время ожидания приоритетного пакета будет равно времени обработки одного пакета, и если эти пакеты небольшого размера, то и отклонение от синхронизма будет небольшое. Введение типов трафика и приоритетное обслуживание являются еще одной особенностью технологии ATM, которая позволяет ей успешно совмещать в одном канале

синхронные и асинхронные пакеты. В сетях ATM соединение конечного узла с сетью осуществляется индивидуальной линией связи, а коммутаторы соединяются между собой каналами с уплотнением, которые передают пакеты всех узлов, подключенных к соответствующим коммутаторам.

Сеть ATM имеет структуру, похожую на структуру телефонной сети - конечные станции соединяются с коммутаторами нижнего уровня, которые в свою очередь соединяются с коммутаторами более высоких уровней. Коммутаторы ATM пользуются адресами конечных узлов для маршрутизации трафика в сети коммутаторов. Коммутация пакетов происходит на основе идентификатора виртуального канала (Virtual Channel Identifier, VCI), назначается соединению при его установлении и уничтожается при разрыве соединения. Виртуальные соединения устанавливаются на основании длинных 20-байтных адресов конечных станций. Такая длина адреса рассчитана на очень большие сети, вплоть до всемирных.

Адрес имеет иерархическую структуру, подобную номеру в телефонной сети и использует префиксы, соответствующие кодам стран, городов и т.п. Виртуальные соединения могут быть постоянными (Permanent Virtual Circuit, PVC) и коммутируемыми (Switched Virtual Circuit, SVC). Постоянные виртуальные соединения соединяют двух фиксированных абонентов и устанавливаются администратором сети. Коммутируемые виртуальные соединения устанавливаются при инициации связи между любыми конечными абонентами. Соединения конечной станции ATM с коммутатором нижнего уровня определяются стандартом UNI (User Network Interface). UNI определяет структуру пакета, адресацию станций, обмен управляющей информацией, уровни протокола ATM и способы управления трафиком.

Стек протоколов ATM. Формат ячейки ATM показан в таблице 1, а стек протоколов ATM – в таблице 2. Стек протоколов ATM соответствует нижним уровням семиуровневой модели ISO/OSI и включает адаптационные уровни ATM, называемые AAL1-AAL5, и собственно уровень ATM. Адаптационные уровни транслируют пользовательские данные от верхних уровней коммуникационных протоколов в пакеты, формат и размеры которых соответствуют стандарту ATM. Каждый уровень AAL обрабатывает пользовательский трафик с определенными характеристиками. Уровень AAL1 занимается трафиком с постоянной битовой скоростью (CBR), который

характерен, например, для цифрового видео и цифровой речи и чувствителен как к потере ячеек, так и к временным задержкам. Этот трафик передается в сетях ATM так, чтобы эмулировать обычные выделенные цифровые линии. Уровень 3/4 обрабатывает пульсирующий трафик с переменной битовой скоростью (VBR), обычно характерный для трафика локальных сетей. Этот трафик обрабатывается так, чтобы не допустить потерь ячеек, но ячейки могут задерживаться коммутатором. Уровень AAL3/4 выполняет сложную процедуру контроля ошибок при передаче ячеек для их гарантированной безошибочной доставки. Уровень AAL5 является упрощенным вариантом уровня AAL4, он работает быстрее.

Введение различных классов сервисов, реализуемых в стеке протоколов ATM адаптационными уровнями AAL, а также самим протоколом ATM, и позволяет реализовать в сетях ATM совместное сосуществование трафиков разной природы. Коммутаторы ATM, получая в поле типа данных ячейки (поле PTI) информацию о классе сервиса, принимает решение о приоритете обслуживания данной ячейки.

Для того, чтобы каждый класс сервиса выполнялся с нужным уровнем качества, в технологии ATM предусмотрены достаточно сложные процедуры заказа качества обслуживания, которые выполняются между станцией и сетью при установлении соединения.

Классы сервиса. В сети ATM каждый раз, когда приложению необходимо установить соединение между двумя пользователями, оно должно заказать вид сервиса, в соответствии с которым будет обслуживать трафик по данному соединению. Классы сервиса ATM содержат ряд параметров, которые определяют гарантии качества сервиса. В спецификациях ATM предусмотрено несколько классов сервиса - CBR, VBR, UBR и ABR (появился совсем недавно). Гарантии качества сервиса могут определять минимальный уровень доступной пропускной способности и предельные значения задержки ячейки и вероятности потери ячейки .

Сервис CBR (constant bit rate, сервис с постоянной битовой скоростью) представляет собой наиболее простой класс сервиса ATM. Когда сетевое приложение устанавливает соединение CBR, оно заказывает пиковую скорость трафика ячеек (peak cell rate, PCR), которая является максимальной скоростью, которое может поддерживать соединение без риска потерять ячейку. Затем

данные передаются по этому соединению с запрошенной скоростью - не более и, в большинстве случаев, не менее. Любой трафик, передаваемый станцией с большей скоростью, может сетью просто отбрасываться, а передача трафика сетью со скоростью, ниже заказанной, не будет удовлетворять приложение. CBR-соединения должны гарантировать пропускную способность с минимальной вероятностью потери ячейки и низкими изменениями задержки передачи ячейки. Когда приложение заказывает CBR сервис, то оно требует соблюдения предела изменения задержки передачи ячейки. Сервис CBR предназначен специально для передачи голоса и видео в реальном масштабе времени. Сервис CBR также подходит для эмуляции цифровых каналов типа T1/E1.

Для соединений CBR нет определенных ограничений на скорость передачи данных, и каждое виртуальное соединение может запросить различные постоянные скорости передачи данных. Сеть должна резервировать полную полосу пропускания, запрашиваемую конкретным соединением. Класс трафика VBR (variable bit rate, сервис с переменной битовой скоростью) включает два подкласса: трафик VBR реального времени (VBR-RT) и трафик VBR не реального времени (VBT-NRT). Трафик VBR-RT допускает очень узкие границы для задержки передачи ячеек и может использоваться для передачи данных приложений реального времени, которые позволяют небольшое изменение задержки передачи ячеек, таких как видео, генерируемое кодеком с переменной скоростью данных или компрессированный видеотрафик, в котором удалены промежутки "молчания". Трафик VBR-NRT в свою очередь предъявляет менее жесткие требования к задержке передачи ячеек. Он специально предназначен для передачи коротких, пульсирующих сообщений, таких как сообщения, возникающие при обработке транзакций системами управления базами данных.

По сравнению с сервисом CBR, VBR требует более сложной процедуры заказа соединения между сетью и приложением. В дополнение к пиковой скорости приложение VBR заказывает еще и другой параметр: длительно поддерживаемую скорость (sustained rate), которая представляет собой среднюю скорость передачи данных, которая разрешена приложению. Пользователь может превышать скорость вплоть до величины PCR, но только на короткие периоды времени, а соединение VBR будет использовать среднее значение SCR

для управления трафиком, снижая его интенсивность на соответствующие периоды времени.

Как и при CBR-соединении, приложение и сеть должны прийти к соглашению относительно пиковой скорости PCR и допустимости задержек передачи ячеек. Но в отличии от CBR, соединение VBR должно установить временной предел - как долго могут передаваться данные на скорости PCR. Когда этот предел, известный как допустимая пульсация, превышается, за ним должен следовать период более низкой активности станции, чтобы обеспечить заданный уровень SCR. Эти периоды низкой активности дают возможность другим видам трафика, таким как ABR, получить доступ к сети.

Как и в случае CBR, пользователи VBR получают гарантированное обслуживание в отношении потерь ячеек, изменения задержек передачи ячеек и доступной полосы пропускания до тех пор, пока трафик удовлетворяет определенным при соединении требованиям. Однако для многих приложений, которые могут быть чрезвычайно "взрывными" в отношении интенсивности трафика, невозможно точно предсказать параметры трафика, оговариваемые при установлении соединения. Например, обработка транзакций и трафик двух взаимодействующих локальных сетей непредсказуемы по своей природе, изменения трафика слишком велики, чтобы заключить с сетью какое-либо разумное соглашение.

В результате администраторы сетей, ответственные за такие приложения, имеют три возможности. Они могут заплатить за дополнительную пропускную способность, которая может оказаться неиспользованной. Они могут попытаться управлять пульсациями трафика более тонко (сложная задача для большинства приложений). Или же они могут превысить скорость, оговоренную при установлении соединения, пренебрегая гарантированным качеством обслуживания.

Для тех, кто выбирает последний вариант, последствия скорее всего будут и самыми тяжелыми - потеря ячеек. Потерянные ячейки должны быть повторно переданы узлом-отправителем. Для ответственных приложений это серьезная проблема, для низкоприоритетных приложений, таких как электронная почта, повторная передача ячеек является досадной потерей времени.

В отличие от CBR и VBR, сервис UBR (unspecified bit rate, неопределенная битовая скорость) не определяет ни битовую скорость, ни

параметры трафика, ни качество сервиса. Сервис UBR предлагает только доставку "по возможности", без гарантий по утере ячеек, задержке ячеек или границам изменения задержки. Разработанный специально для возможности превышения полосы пропускания, сервис UBR представляет собой частичное, но неадекватное решение для тех непредсказуемых "взрывных" приложений, которые не готовы согласиться с фиксацией параметров трафика. Главными недостатками подхода UBR являются отсутствие управления потоком данных и неспособность принимать во внимание другие типы трафика. Когда сеть становится перегруженной, UBR-соединения продолжают передавать данные. Коммутаторы сети могут буферизовать некоторые ячейки поступающего трафика, но в некоторый момент буфера переполняются и ячейки теряются. А так как UBR-соединения не заключали никакого соглашения с сетью об управлении трафиком, то их ячейки отбрасываются в первую очередь. Потери ячеек UBR могут быть так велики, что "выход годных" ячеек может упасть ниже 50%, что совсем неприемлемо.

Сервис ABR (available bit rate), подобно сервису UBR, использует превышение полосы пропускания, но он использует технику управления трафиком для оценки степени переполнения сети и избегает потерь ячеек. ABR - это первый класс сервиса технологии ATM, который действительно обеспечивает надежный транспорт для приложений с пульсирующим трафиком за счет того, что он может находить неиспользуемые интервалы времени в трафике и заполнять их своими пакетами, если другим классам сервиса эти интервалы не нужны .

ЛИТЕРАТУРЫ:

1. "Эко-Трандз". Цифровая телефония. Беллами Д.К., 2017
2. Нессер Дж. Оптимизация и поиск неисправностей в сетях. - Киев: Диалог, 2016
3. Сибаров Ю.Т., Сколотов Н.А. Охрана труда в ВЦ. М.: Машиностроение, 2014
4. Максимов Д.К., Шиндаулетова А.Т. Расчет экономической эффективности внедрения курсовых работ и дипломных проектов. Методические указания. - Алматы: КазНТУ, 2017

Počítače a programování

Пархоменко І.І.,
к.т.н., доцент, parkh08@ukr.net
Носенко Ю.В.,
магістр НАУ nosenko.yur@gmail.com

ЗАХИСТ WEB - ДОДАТКІВ В МЕРЕЖІ ІНТЕРНЕТ

Безсумнівно, інтернет-сервіси несуть з собою безліч переваг, але є й зворотна сторона медалі – з ростом числа додатків збільшується і кількість кіберзагроз. Згідно зі статистикою (рис. 1), вразливості авторизації широко поширені, часто мають високий рівень небезпеки, а сучасні автоматизовані засоби пошуку вразливостей веб-ресурсів не дозволяють ефективно виявляти всі проломи системи [1].

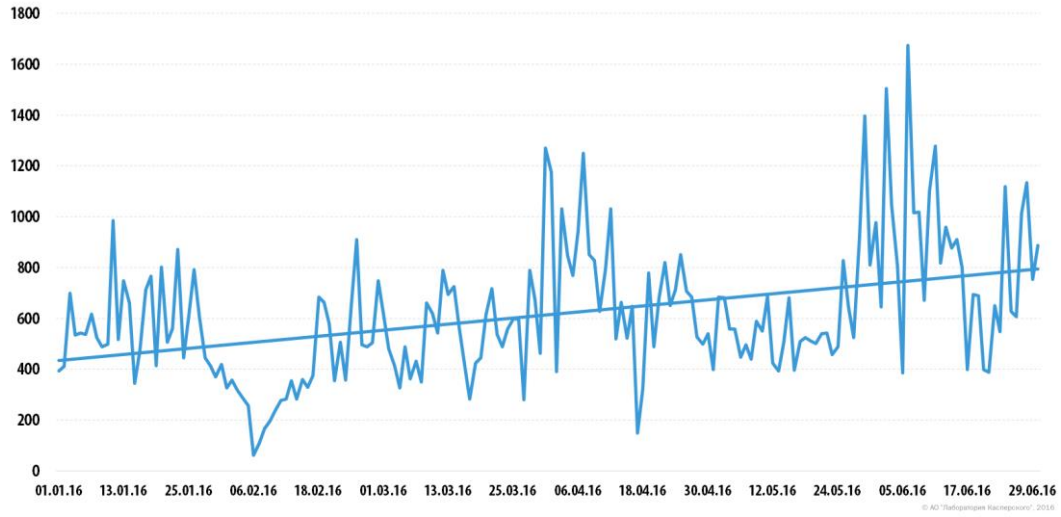


Рисунок 1 – Динаміка атак на веб-ресурси в першому та другому кварталі 2016 року.

Як тільки веб-додаток стає доступним в мережі, він стає мішенню для кібератак. Незалежно від того, чи здійснюється атака цілеспрямовано зловмисниками або є результатом роботи автоматизованого шкідливого програмного забезпечення, будь-який веб-додаток буде постійно перевірятися на міцність з усіх боків. Отже, перш ніж починати використовувати свої веб-ресурси, необхідно забезпечити їм надійний захист,

одним з яких є розмежування доступу основаного на методі «чорного ящика» [2]. При дослідженні веб-додатків методом «чорного ящика» використовується гіпотеза про те, що призначений для користувача інтерфейс повинен відображати його права: дозволені користувачу дії присутні в його веб-інтерфейсі, а заборонені, навпаки, відсутні. Всі існуючі засоби пошуку вразливостей авторизації методом чорного ящика використовують метод «аналізу відмінностей» [3]. Відповідно до цього методу, для кожного з користувачів будується «карта сайту» - безліч ресурсів, доступних користувачеві через його інтерфейс. Далі для кожної пари користувачів проводиться спроба доступу до ресурсів одного користувача від імені іншого. Такий підхід має ряд проблем, що обмежує його застосування. Головною з яких є те, що розглянутий метод не враховує стан веб-додатка як при побудові карт сайту, так і при проведенні тестів. Це призводить до неповної побудови карт і виявлення вразливостей.

Для подолання цього обмеження в пропонованому методі процедура, «аналізу відмінностей» застосовується в декількох спеціально підібраних станах. При цьому етап побудови карт сайту модифікований таким чином, щоб забезпечити незмінність стану веб-додатку. Стану, в якому відбувається аналіз, будуються таким чином. Замість HTTP-запитів до додатка розглядаються сценарії використання, які відображають дію відповідну запиту, і роль користувача, що здійснює запит. Оператор вручну ідентифікує сценарії використання і задає залежності між ними. Отриманий граф сценаріїв використання обходиться з урахуванням залежностей. На кожному кроці переходу відбувається дія, відповідна поточній вершині, і проводиться аналіз відмінностей в отриманому стані. Друга проблема виникає при побудові карт сайту для сучасних веб-додатків. Головною підзадачею при цьому є отримання для даної сторінки безліч запитів, які можуть бути здійснені в результаті дій користувача. Для класичних веб-додатків завдання тривіально вирішується виділенням на сторінці посилань і веб-форм, тоді як в веб-додатках з динамічними інтерфейсами необхідно аналізувати javascript-програми, впроваджені в HTML-код сторінки.

Суть пропонованого підходу полягає в збуджені подій для елементів сторінки і перехопленні HTTP-запитів (рис. 2). Для прискорення аналізу були враховані особливості бібліотеки jQuery, що дозволило шляхом динамічного

аналізу контексту виконання знизити безліч тестованих елементів. Запропоновані ідеї були реалізовані у вигляді набору інструментальних засобів пошуку вразливостей авторизації. При цьому крім запропонованого методу був також реалізований існуючий метод, що дозволило зробити їх експериментальне порівняння. Порівняння виявило збільшення повноти пропонованого методу в порівнянні з існуючим при кількості помилкових спрацьовувань.

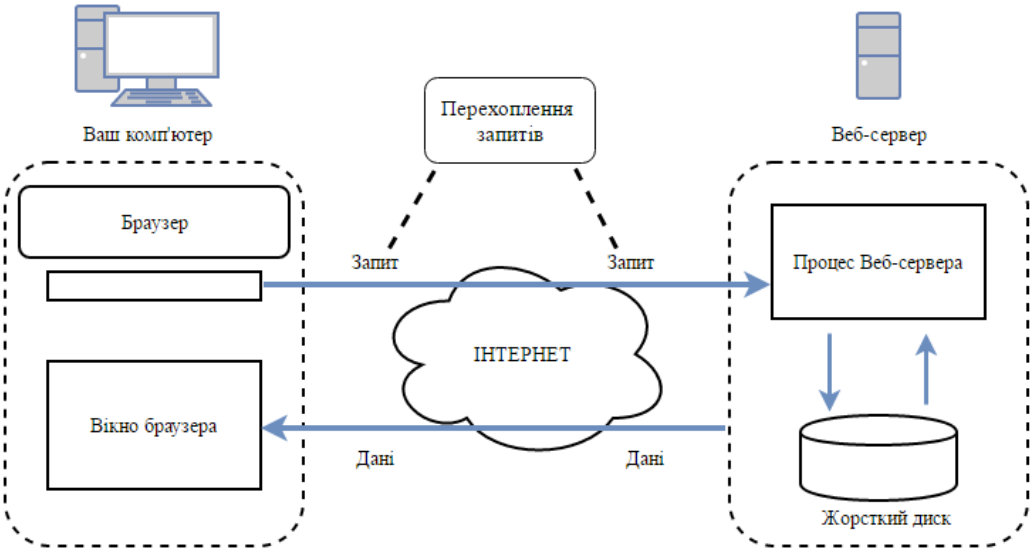


Рисунок 2 – Перехоплення HTTP-запитів при збуджені подій елементів сторінки.

Нехтування питаннями захисту веб-ресурсів може критично позначитися на роботі веб-сайту. Навіть просте спотворення сторінки може привести до несприятливої думки в засобах масової інформації і вдарити по репутації, однак найчастіше атаки зловмисників націлені на викрадення персональних даних, що є найбільш вигідним для них і при цьому завдає найбільшої шкоди потерпілій стороні. У разі серйозного витоку даних ви отримуєте безліч прихованих витрат: судові розслідування, простої і переписування коду веб-сайту. Все це має дуже високу ціну.

Список використаних джерел

1. Пенцак Т.О., Носенко Ю.В “ ЗАХИСТ WEB - РЕСУРСІВ ВІД ШКІДЛИВОГО КОДУ” / Вісник інженерної академії України випуск – 2017 – С. 3-4.

2. Web Application Security Consortium. Web application security statistics 2008. http://projects.webappsec.org/f/WASS-SS-2008.pdf.
3. Segal O. Automated Testing of Privilege Escalation in Web Applications, Watchfire, 2006.
4. Пархоменко І.І., Воскобойніков А.О., "Організація захищеної передачі даних в системі Web-сервер – клієнт" / Вісник інженерної академії України випуск – 2014 – С. 116-120.
5. Фролов А. В. Бази даних в Мережі інтернет: Практичний посібник по створенню Web-додатків з базами даних / А. В. Фролов., 2000. – 448 с.

Software

Айдосов А., Заурбеков Н.С., Заурбекова Г.Н., Кзылбаев М.С., Аппакова А.А.

(Алматинский технологический университет, Казахский национальный университет имени аль-Фараби, Алматы, Республика Казахстан)

МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ ДИНАМИКИ ВЕРТИКАЛЬНЫХ ДВИЖЕНИЙ В ОБЛАЧНОЙ АТМОСФЕРЕ ДЛЯ ОЦЕНКИ КАЧЕСТВА ВЕРТИКАЛЬНЫХ ДВИЖЕНИИ И ЧИСТОТЫ АТМОСФЕРНОГО ВОЗДУХА

В практике отсутствует методы измерения в мезомасштабных процессах атмосферы метеорологического параметра вертикальные движения, поэтому мы теоретически обоснуем пути определению вертикальных движений. Благодаря вертикальным движениям происходит процессы переноса водяного пара, конденсации в атмосфере. А с конденсацией тесно связаны облакообразования и осадки в атмосфере, поэтому их можно использовать для оценки качества вертикальных движении и чистоты атмосферного воздуха.

Проблема учета вертикальных скоростей впервые изложены в работах Н.И.Булеева и Г.И.Марчука [1] и Хинкельмана [2], Бурцев А.И. [3], Шершков В.В. [4], где вертикальная скорость (а точнее $\omega = \frac{dP}{dt}$) находится из решения эллиптического уравнения, в правой части которого имеются источники, вызываемые распределением адвекции вихря и температуры. Многие авторы отмечают вертикальные скорости как важный бароклинный параметр [1, 5-12], определяющий перераспределение потенциальной и кинетической энергии в вертикальном направлении.

Ф.Томпсон впервые обратил внимание, что из системы уравнений, включающей уравнения неразрывности, притока тепла, состояния и гидростатики можно построить довольно точно описываемое балансовое уравнение в декартовых координатах. Например, для состояния сухой атмосферы это соотношение:

$$\frac{\partial}{\partial z} P \frac{\partial W}{\partial z} = -\frac{\partial}{\partial z}(PD) + \frac{1}{\chi}\frac{\partial P}{\partial z} D + \frac{1}{\chi}\frac{\partial}{\partial z}\left(P \frac{\tilde{\varepsilon}}{C_P} \right) + \frac{pB}{\chi}, \quad \text{где} \quad D = \frac{\partial U}{\partial x} + \frac{\partial V}{\partial y}.$$

При условиях z=0, $W = W_0(x,y)$, $z \to \infty$, $p \to 0$

интегрирование и решение этого уравнения не вызывает трудностей.

Для вертикальной скорости в насыщенной атмосфере получим модели введя в них диссипативные члены ε_θ, ε_π и ε_m, описывающее баланс между вертикальными движениями, горизонтальной бароклинностью, плоской дивергенцией и притоками тепла:

$$\frac{\partial}{\partial z}\varphi_1 \frac{\partial W}{\partial z} + \mu \frac{\partial \ln P}{\partial z}\frac{\partial W}{dz} = -\frac{1}{\chi} B - \frac{\partial}{\partial z}\left(\varphi_1 D - \varphi_2 \frac{\tilde{\varepsilon} + \varepsilon_\pi}{C_P} \right) -$$

$$-\frac{\partial \ln P}{\partial z}\left((\mu\varphi_1 - \frac{1}{\chi}) D_2 - (\mu\varphi_2 - \frac{\nu}{\chi})\frac{\tilde{\varepsilon}}{C_P} + (\frac{\nu_1}{\chi} - \mu\varphi_2)\frac{\varepsilon_\pi}{C_P} - \frac{\nu_2\varepsilon_\theta}{\chi C_P} - \frac{\nu_3\varepsilon_m}{\chi C_P} \right), \qquad (1)$$

где $divV = D + \frac{\partial W}{\partial z}$, $D_2 = D + I^*$.

Здесь все члены, кроме W, известны.

Краевые условия: на верхней границе при $z \to \infty$ $\frac{dP}{dt} \to 0$, или $p \to 0$;

на нижней границе: z=0, $W = W_0(x,y)$, если земля плоская W_0=0.

Умножая на p^{μ/φ_1} уравнение (1), получим после несложных преобразований следующее уравнение, легко решаемое с помощью квадратуры с учетом краевых условий:

$$\frac{\partial}{\partial z}\varphi_1 p^{\mu/\varphi_1}\frac{\partial W}{\partial z} = p^{\mu/\varphi_1} F,$$

где F – правая часть уравнения (1).

Исключая плотность из модели неразрывности и полагая α_3=0, m^*=m и I^*=0, модели притока тепла разделив на βp, логарифмируя и интегрируя от 0 до Z, получим:

$$W = W_0(x,y) - \int_0^\infty \left[G_D(z,z')D - \frac{1}{\chi} G_B(z,z')B \right] dz' + \int_0^Z \left[\frac{\tilde{\varepsilon}}{C_P(1+1{,}83\chi m)} + \frac{\tilde{\sigma}}{\beta}\frac{d\ln(1+m)}{dt} \right] dz',$$

где $\beta = \frac{1+1{,}83m}{1+1{,}83\chi m}$, $\tilde{\sigma} = \frac{1}{1{,}83\chi m}\left(0{,}606\beta - \frac{\chi - 1}{\chi}\frac{1}{0{,}623 - 0{,}378m} \right)$;

$$G_B = \delta\sigma(z') + (1-\delta)\sigma(z)\frac{P(z')}{P(z)}, \qquad G_D = \delta(1-\frac{g\sigma(z')}{\chi RT(z')}) - (1-\delta)\frac{g\sigma(z)}{\chi RT(z')}\frac{P(z')}{P(z)}.$$

G_D, G_B – функции Грина для Z=1, 5, 6 и 12 км. Отметим, что функции Грина почти не отличаются от функции Грина, предложенные нами для сухой атмосферы.

Хотя эти функции мало отличаются друг от друга, отметим некоторые их особенности, вытекающие из вида функции. В сравнении четко заметно влияние сжимаемости: во всей толще атмосферы дивергенция оказывает заметное влияние на величину вертикальной скорости. То есть, можно сделать вывод: чем больше высота Z, тем больше эффект самых верхних уровней на величину вертикальной скорости. Аналогично и с горизонтальной бароклинностью и турбулентным потоком тепла, их влияние также проявляется сильнее на больших высотах. Это объясняется тем, что, как следует из полученного нами вида функции Грина для W, турбулентный поток энергии влияет на вертикальные движения подобно дивергенции.

Как известно, при безоблачной атмосфере единственным механизмом, регулирующим перераспределение влажности в пространстве, является турбулентный обмен [1,10]. Выпишем уравнение переноса отношения смеси, с учетом вышесказанного, добавляя к нему свойства турбулентного обмена:

$$\frac{dm}{dt} = K_h\Delta m + \frac{\partial}{\partial z}K\frac{\partial m}{\partial z},$$

где K, K_h – коэффициенты турбулентного обмена в вертикальном и горизонтальном направлениях. Пусть ΔW_h - вклад изменений влажности в вертикальные движения слоя толщиной Z-Z_1, тогда зная, что $\frac{\tilde{\sigma}}{\beta}\frac{1}{1+m} \approx 0{,}2$, его можно представить в приближенном виде:

$$\Delta W_h \approx 0{,}2\left[K\frac{\partial m}{\partial z}|_{Z_1}^{Z} + (z-z_1)K_h\Delta\tilde{m}\right],$$

где $\tilde{m}$ – среднее соотношение смеси в слое Z-Z_1.

Отметим, что первое слагаемое зависит от характера вертикального распределения отношения смеси и с увеличением высоты кривая распределения влажности довольно резко убывает, поэтому в районе перелома наблюдается дополнительные приращения W, и они направлены вниз.

Анализ и количественные оценки дают сделать вывод, что величина ΔW_h порядка 1 мм/с, то есть очень малы в практическом смысле. Однако, надо учесть, что для него довольно длительное время существует благоприятное условие и эти малые величины могут оказать заметное влияние.

Литература

1. Булеев Н.И., Марчук Г.И. О динамике крупномасштабных атмосферных процессов // Тр. ИФА АН СССР. – 1958. – №2.
2. Хинкельман К.Г. Полные уравнения. Лекции по численным методам краткосрочного прогноза погоды. – Л.: Гидрометеоиздат, 1969. – С.317-371
3. Бурцев А.И. Метод расчета вертикальных скоростей воздуха при учете изменения вертикального градиента температуры с высотой // Тр. ЦИП. – Вып.77. – 1958.
4. Шершков В.В. Некоторые вопросы задачи вынужденной конвекции в пограничном слое атмосферы // МиГ. – 1969. – №1. – С.36-41
5. Иорданов Д.Л., Паненко В.В., Алоян А.Е. О вертикальной скорости на верхней границе планетарного пограничного слоя над орографически и термически неоднородной подстилающей поверхностью // Изв. АН СССР. Сер.: ФАО. Т.15. Сер. II. – 1979. – №11. – С. 1204-1208.
6. Айдосов А., Заурбеков Н.С. Теоретические основы прогнозирования природных процессов и экологической обстановки окружающей среды. - А., ҚазНУ, 2000.. – 219 с.
7. Айдосов А., Айдосов Г.А., Заурбеков Н.С. Модели экологической обстановки окружающей среды при реальных атмосферных процессах- Алматы, 2010 – 368 с.
8. Айдосов А. и др. Модели прогноза изменений качества компонентов природной среды южных промышленных регионов от техногенной нагрузки и их влияния на показателей изменения здоровья населения - Алматы, 2016. – 240 с.

9. Айдосов А., Заурбеков Н.С. Модели и методы оценки влияния вредных веществ на компоненты природных сред - Монография /Алматы, 2016. - 252 с.
10. Айдосов А., Айдосов Г.А., Заурбеков Н.С. Теория и методы описания распространения естественных и антропогенных загрязнений при различных климатических условиях - Алматы, 2016. - 240 с.
11. Айдосов А., Айдосов Г.А. Заурбеков Н.С. Теоретические основы исследования состояния компонентов природных сред и методы оценки влияния естественных и антропогенных нагрузках - Монография / Алматы, 2017, - 232 с.
12. Айдосов А., Айдосов Г.А. Заурбеков Н.С. Модельная оценка экологической обстановки компонентов природной среды с учетом атмосферных процессов - М.: Издательский дом Академии Естествознания, 2018. – 342 с.

Пархоменко І.І.,
д.т.н.,проф., parkh08@ukr.net
Чигринюк В.Ю.,
магістр НАУ, vladchugrunyuk@gmail.com

ЗАХИСТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

Для ефективної роботи підприємства необхідно спланувати й побудувати корпоративну мережу, а також зробити оптимальний вибір технічних засобів, що становлять основу мережі. Тому питання захисту інформації стало невід'ємною частиною любої системи яка працює з різного роду інформацією, яка б не повинна була втратити свою конфіденційність. При використанні Internet в комерційних межах а також для з'єднання частин компаній і організацій, виникають проблеми захищеності інформації яка проходить через мережу. Захист даних в мережі, можна поставити на перше місце при проектуванні корпоративних мереж.

Міжмережевий екран (МЕ) називають локальний або функціонально розподілений програмний (програмно-апаратний) засіб (комплекс), який реалізує контроль за інформацією, що надходить в автоматизовану систему або виходить з автоматизованої системи. Також зустрічаються загальноприйняті назви брандмауер і firewall.

Рис.1. Схема фільтрації в МЕ

Система забезпечення безпеки інформації повинна мати багаторівневу структуру і включати наступні рівні:

рівень захисту автоматизованих робочих місць (АРМ);

рівень захисту локальних мереж та інформаційних серверів;

рівень захисту корпоративної АС.

На рівні захисту автоматизованих робочих місць повинна здійснюватися ідентифікація та аутентифікація користувачів операційної системи. Повинно здійснюватися управління доступом: надання доступу суб'єктів до об'єктів відповідно до матрицею доступу, виконання реєстрації та обліку всіх дій суб'єкта доступу в журналах реєстрації. Повинна бути забезпечена цілісність програмного середовища, періодичне тестування засобів захисту інформації.

Рівень захисту локальних мереж і мережевих серверів повинен забезпечувати:

ідентифікацію користувачів і встановлення автентичності доступу в систему, до компонентів;

захист аутентифікаційних даних;

встановлення аутентичності при доступі до серверів;

Для побудови корпоративної мережі, яка включає в себе локально розмежовані підмережі, слід приділяти велику увагу контролю цілісності передачі даних, та унеможливлення зовнішніх проникнень в самі мережі чи в канали зв’язку між ними.

Забезпечення захисту інформаційної структури

Успіх виробничої і підприємницької діяльності в чималому ступені залежить від уміння розпоряджатися таким найціннішим товаром, як інформація, але вигідно використовувати можна лише ту інформацію, яка потрібна ринку, але невідома йому. Тому в умовах посилення конкуренції успіх підприємництва, гарантія отримання прибутку все більшою мірою залежать від збереження в таємниці секретів виробництва, що спираються на певний інтелектуальний потенціал і конкретну технологію.

Підприємницька (комерційна) діяльність тісно пов'язана з отриманням, накопиченням, зберіганням, обробкою і використанням різноманітних інформаційних потоків. Однак захисту підлягає не вся інформація, а тільки та, яка представляє цінність для підприємця. При визначенні

цінності підприємницької інформації необхідно керуватися такими критеріями (властивостями), як корисність, своєчасність і достовірність надійшли відомостей.

Розробку заходів щодо збереження комерційної таємниці підприємства слід здійснювати, дотримуючись принцип комплексного перекриття можливих каналів витоку інформації та забезпечення рівнозначної надійності захисту всіх її носіїв. Загрози збереження комерційної таємниці можуть бути зовнішніми і внутрішніми.

Питання захисту інформаційних систем актуальний тільки тоді, коли існуючі файли не призначаються для загального огляду. Існують таке поняття, як захист інформаційних систем, яке розділяється на рівні безпеки. Інформація може бути загальнодоступною чи доступною тільки обмеженому колу людей.

Література

1. Захист об’єктів інформаційно-комунікаційної структури підприємства/С. В. Толюпа, В. Ю. Чигринюк. – 2017р.
2. Захист інформації в розподілених корпоративних мережах і системах / А. В. Соколов, В. Ф. Шаньгина. - ДМК Прес., 2012. - 656с.
3. Безпека підприємницької діяльності / Крисін В.А. - М: Фінанси і статистика, 2010р.
4. Аналіз захищеності корпоративних автоматизованих систем / А. Астахов. – 2010р. – 121с.
5. Безпечне управління ресурсами та користувачами в корпоративних інформаційних мережах/ Емінов Б.Ф., Еміне Ф.І.: Навчальний посібник. - К.: ЗАТ «Нове знання», 2006.

Informační bezpečnost

Мелешко О. О., доц.; Голишевська І.В., студентка
Національний авіаційний університет, Київ

СПОСОБИ ВИЯВЛЕННЯ ТА ЗАХИСТУ ВІД ШКІДЛИВИХ ПРОГРАМ

Шкідлива програма (ШП) – це комп'ютерна програма або переносний код, призначений для реалізації загроз інформації, що зберігається в комп'ютерній системі, або для прихованого нецільового використання ресурсів системи, або іншої дії, що перешкоджає нормальному функціонуванню комп'ютерної системи.

Проблема ШП загострюється з кожним роком, проте останнім часом змінилися цілі їх розробки і застосування, що обумовлює деякі особливості сучасних ШП, і, як наслідок, вимагає наявності в антивірусних програмних засобах відповідних механізмів боротьби з ними. Якщо в недавньому минулому ШП розроблялися вузьким колом фахівців, а цілі їх розробки були вельми туманні, то зараз переважна більшість ШП розробляється з метою отримання фінансової вигоди. Найбільш поширені класи сучасних ШП наступні:

Троянські програми - використовуються для розкрадання конфіденційної інформації.

Черви з троянськими компонентами - на їх основі створюються керовані розподілені мережі, які використовуються для розсилки спаму і розподілених мережевих атак.

AdWare (рекламне ПЗ) – використовується для показу рекламних повідомлень на комп'ютері.

SpyWare (шпигунське ПЗ) - програма, яка потайним чином встановлюється на комп'ютер з метою повного або часткового контролю за роботою комп'ютера і користувача без згоди останнього.

Для протидії ШП використовуються антивірусні програми. Найбільш розповсюджений спосіб виявлення ШП - сигнатурний пошук. Цей метод виявлення застосовується антивірусними програмами в першу чергу. Він

реалізовується шляхом перевірки вмісту аналізованого об'єкта на предмет наявності в ньому сигнатур вже відомих загроз. Сигнатурою називається безперервна кінцева сукупність електронних даних, необхідна і достатня для однозначної ідентифікації загрози. При цьому порівняння вмісту досліджуваного об'єкта з сигнатурами проводиться не безпосередньо, а за їх контрольними сумами, що дозволяє значно знизити розмір записів у вірусних базах, зберігши при цьому однозначність відповідність і, отже, коректність виявлення загроз і лікування інфікованих об'єктів. Недоліком цього способу є необхідність постійного оновлення баз сигнатур.

Для боротьби з модифікацією ШП на рівні вихідного коду в сучасному антивірусному ПО використовується такий механізм, як евристичний аналізатор. В даному методі його робота грунтується на наборі евристик (припущень, статистична значимість яких підтверджена дослідним шляхом) про характерні ознаки шкідливого і, навпаки, безпечного виконуваного коду. Кожна ознака коду має певне політичне значення (тобто число, що показує важливість і достовірність цієї ознаки). Вага може бути як позитивною, якщо ознака вказує на наявність шкідливої поведінки коду, так і негативною, якщо ознака не властива комп'ютерним загрозам. На підставі сумарної ваги, що характеризує вміст об'єкта, евристичний аналізатор обчислює ймовірність вмісту в ньому невідомого шкідливого об'єкта. Якщо ця ймовірність перевищує деяке порогове значення, то видається висновок про те, що аналізований об'єкт є шкідливим.

Недоліком цього методу є те, що дуже часто мають місце випадки помилкового спрацьовування, при чому доволі часто вони перевищують кількість вірних.

Іншим методом є емуляція виконання програмного коду. Даний спосіб використовується для виявлення поліморфних і шифрованих вірусів, коли використання пошуку по контрольних сумах сигнатур не застосовується або значно ускладнено через неможливість побудови надійних сигнатур. Метод полягає в імітації виконання аналізованого коду за допомогою емулятора - програмної моделі процесора і середовища виконання програм. Емулятор оперує з захищеною областю пам'яті (буфером емуляції). При цьому інструкції не передаються на центральний процесор для реального виконання. Якщо код, що обробляється емулятором, інфікований, то результатом його емуляції стане відновлення вихідного шкідливого коду, доступного для сигнатурного аналізу.

Цей шлях є найбільш перспективним, оскільки дозволяє підтримувати широкий спектр існуючих і розроблених в майбутньому пакувальників (крипторів), але одночасно пред'являє високі вимоги до швидкодії емулятора. Необхідні модифікації емулятора при такому підході полягають в його доопрацювання з метою додавання емуляції додаткових функцій або структур ОС. Якісні зміни в цьому напрямку відбуваються доволі рідко, оскільки розробка таких алгоритмів доволі трудомістка та витратна.

На сьогоднішній день кількість ШП стрімко збільшується, тому, відповідно, розробляється багато нових способів виявлення та захисту від них. Використання передових технологій боротьби дозволяє ефективно виявляти не тільки існуючі ВП, а й запобігати вірусні атаки, що використовують нові ВП.

Література

1. Безруков, Н.В. Комп’ютерна вірусологія: Підручник [Електронний ресурс]. – Режим доступу: http://vx.netlux.org/lib/anb00.html.
2. Фролов А.М. Обережно, комп’ютерні віруси[Текст] / Фролов А.М. – М.: Диалог-МИФИ, 2005. – 256 с.
3. Технології боротьби зі шкідливим ПО [Електронний ресурс]. – Режим доступа: https://hackzona.ru/articles/164-texnologii-borby-s-vredonosnym-po.html
4. Таненбаум, Э. Современный операционные системы [Текст] / Э. Таненбаум – К.: С-Пптер, 2003. – С.582.

К.т.н., доцент Ільєнко А.В., Радик Т.В.
Національний авіаційний університет (НАУ), Україна

ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ІНФОРМАЦІЇ З ВИКОРИСТАННЯМ ПОНЯТТЯ «ЦИФРОВОГО КОНВЕРТУ»

Вступ. Проблеми в області безпеки інформації набули виключної актуальності за останні роки, при цьому забезпечення захисту в сфері інформаційних технологій приймає комплексний характер. Існує багато різних методів захисту інформації: правових, організаційних, технічних та інших. Проте, найважливіше місце займають саме криптографічні методи.

Постановка задачі. Метою даної публікації є розкриття криптографічного методу захисту інформації, а саме використання «цифрового конверту».

На сьогоднішній день існує величезна кількість криптографічних алгоритмів, що відрізняються як характеристиками, так і принципами, на яких базується їх робота. Не всі вони є однаково надійними, тому при розробці криптографічного алгоритму необхідно враховувати тенденції розвитку комп'ютерної техніки а також інші фактори, що потенційно можуть знизити його стійкість у майбутньому.

Традиційний метод шифрування, що застосовується при організації захисту даних, які базується на факті знання і використання відправником та адресатом повідомлення одного й того ж секретного ключа. У випадку компрометації ключа стає можливим несанкціонований доступ до даних, тому для надійного функціонування системи необхідна його періодична заміна.. Сукупність заходів по створенню (генерації), передачі та зберіганню ключів носить назву адміністрування ключів (АК).

Для вирішення проблем, пов'язаних із АК, Уітфілдом Діффі та Мартіном Хелманом була запроваджена концепція системи шифрування з відкритим ключем, яка виключає необхідність користувачам ділитись секретною інформацією. Для пересилання конфіденційного повідомлення відправник

шифрує його текст за допомогою відкритого ключа адресата, після чого відсилає за місцем призначення, а адресат розшифровує отриману інформацію, застосовуючи свій секретний ключ [1]. Таким чином, будь-хто може прийняти "чуже" повідомлення, але тільки безпосередній адресат може його прочитати.

Однією з переваг системи шифрування з відкритим ключем є відсутність необхідності покладання на безпеку засобів комунікацій, оскільки між абонентами передаються лише відкриті ключі. Недоліком в порівнянні з системою шифрування з секретним ключем є недостатня швидкість функціонування методу [1].

Попри доцільність окремого застосування кожного із методів при забезпеченні певних типів захисту інформації, в інформаційно-обчислювальних мережах часто застосовується комбінація обох систем для сполучення таких їх позитивних якостей, як швидкість обробки секретних ключів та безпека передачі відкритих. Реалізація такого протоколу "**цифрового конверта**" передбачає шифрування відкритим ключем секретного, який, в свою чергу, використовується для шифрування тексту повідомлення. Таким чином, обидва підходи при застосуванні в розподілених інформаційних середовищах є взаємодоповнюючими в забезпеченні конфіденційного обміну інформацією.

Схема «**цифрового конверту**» являється комбінацією криптосистеми RSA із симетричною криптосистемою, наприклад з алгоритмом DES, TripleDES або AES. Така комбінація представляє собою схему безпечного перехідника.

З точки зору організації протоколу гібридна схема дуже проста. Але існує два обмеження. По-перше, ця схема використовує сеансовий ключ, створений однією із, а інша сторона повинен цілком покладатися на компетентність і чесність ініціатора протоколу [2].

По – друге, гібридні схеми шифрування інертні. В таких системах перехоплювач, який може силою змусити отримувача розкрити свій закритий ключ, отримує можливість розшифрувати усі повідомлення [2].

Ці обмеження можна подолати, якщо в якості криптосистеми з відкритим ключем використовувати протокол обміну ключами Діффі – Хеллмана.

Розглянемо спочатку, як подолати перше обмеження. При запуску протоколу обміну ключами Діффі–Хеллмана між Алісою та Бобом розподілений секрет g^{ab} представляє собою випадкове число, сформоване обома сторонами:

вклад Аліси – число a, вклад Боба – число b. Якщо число g породжує групу, яка має простий порядок, і повідомлення протоколу задовольняють умовам g^a != 1 I g^b !=1, Аліса (відповідно Боб) може бути впевненою, що загальний сеансовий ключ, обчислений на основі g^{ab}, являється випадковим, оскільки вона використала випадковий покажчик степеню [3].

Тепер розглянемо, як зняти інше обмеження. Маємо на увазі, що гібридна схема із протоколом Діффі – Хеллмана володіє властивістю завчасної секретності. Щоб прийняти усі міри обережності, Аліса і Боб повинні обмінятися сеансовим ключем g^{ab}, а після цього стерти покажчики a і b до закінчення протоколу [3]. Також вони повинні знищити сеансовий ключ після закінчення сеансу зв'язку і правильно розмістити вихідні повідомлення, якими вони обмінювались. Якщо вони виконують ці стандартні процедури, то перехоплювач не зможе зламати вихідні дані, якими Аліса та Боб обмінювались. Криптоаналітики також не зможуть впоратись з цією задачею, оскільки властивість завчасної секретності являється засобом наслідком нерозв'язності обчислювальної проблеми Діффі - Хеллмана.

Висновок. З описаного вище можна стверджувати, що використання гібридної схеми шифрування є дуже надійним та ефективним способом захисту інформації (за допомогою протоколу обміну ключами Діффі – Хелламана), якщо її використовувати правильно. Дані гібридні схеми є відносно новими засобами захисту інформації. Особливо можна розробити гібридну схему шифрування яка буде володіти доказовою стійкістю в сенсі сильної стійкості.

Література

1. Брюс Шнайер. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на Си. – М.: Издательство ТРИУМФ, 2002.
2. А. Ю. Нестеренко, А. В. Пугачев, Об одной схеме гибридного шифрования, ПДМ, 2015, номер 4, 56–71.
3. Т. Кормен, Ч. Лейзерсон, Р. Ривест. Алгоритмы: построение и анализ. – М.: МЦНМО, 2002.

К.т.н., доцент Ільєнко А.В., Горобець В. О.
Національний авіаційний університет (НАУ), Україна

ПРОГРАМНІ АСПЕКТИ ЗАХИСТУ НОСІЇВ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ НА ОСНОВІ КРИПТОГРАФІЧНИХ ПЕРЕТВОРЕНЬ

Вступ. В наш час засоби криптографічного захисту інформації (ЗКЗІ) є важливою складовою при забезпеченні інформаційної безпеки, які дозволяють гарантувати високий рівень збереження даних, навіть в разі потрапляння зашифрованих електронних документів в руки третіх осіб, а також при крадіжці або втраті носіїв інформації з ними. ЗКЗІ застосовують сьогодні майже в кожної компанії - частіше на рівні взаємодії з автоматизованими банківськими системами і державними інформаційними системами; рідше - для зберігання корпоративних даних і обміну ними. Тим часом, саме останнє застосування засобів шифрування дозволяє захистити бізнес від небезпечних витоків критично цінної інформації з гарантією до 99% навіть з урахуванням людського фактору.

Постановка задачі. Метою даної публікації є аналіз теоретичних аспектів захист носіїв конфіденційної інформації на основі криптографічних перетворень.

Шифрування носіїв інформації це відомий спосіб захисту проти розкрадання даних. Багато хто вважає, що системи шифрування носіїв інформації дозволять захистити їхні дані, навіть в тому випадку, якщо зловмисник отримав фізичних доступ до комп'ютера (власне для цього вони і потрібні).

Методи програмного захисту, реалізовують підходи до захисту авторських прав, засновані на протидії або створенні копій програм, спробам запуску і виконання незаконної копії. Перевагами володіє програмний захист такої складності, при якій порушник для злому захисту повинен затратити кошти (матеріальні і тимчасові), незрівнянні із засобами, необхідними на придбання програмного продукту або створення власного коду. Говорячи іншими словами, надійним є такий програмний захист, який для злому або обходу механізму захисту, де порушнику необхідно володіти високим потенціалом нападу, тобто

мати високу кваліфікацію, вміти користуватися трудовими і тимчасовими ресурсами.

В даний час спостерігається різке зростання об’ємів інформації (у тому числі і конфіденційної), яка передається по відкритих каналах зв'язку. Тому все більш актуальнішою стає проблема захисту переданої інформації. Незважаючи на те, що конкретні реалізації систем захисту інформації можуть істотно відрізнятися одна від одної через розходження методів і алгоритмів передачі даних, усі вони повинні забезпечувати рішення триєдиної задачі:

конфіденційність інформації (доступність її тільки для того, кому вона призначена);

цілісність інформації (її достовірність і точність, а також захищеність від навмисних і ненавмисних перекручувань);

готовність інформації (використання в будь-який момент, коли в ній виникає необхідність).

Криптографічний захист у більшості випадків є більш ефективним і дешевим. Конфіденційність інформації при цьому забезпечується шифруванням переданих документів або самого носія.

Процес криптографічного захисту даних може здійснюватися як програмно, так і апаратно. Апаратна реалізація відрізняється істотно більшою вартістю, однак їй властиві і переваги це - висока продуктивність, простота, захищеність і т.д. Програмна реалізація більш практична, допускає значну гнучкість у використанні. Перед сучасними криптографічними системами захисту інформації ставлять наступні вимоги:

зашифроване повідомлення повинне піддаватися читанню тільки при наявності ключа;

число операцій, необхідних для визначення використаного ключа шифрування по фрагменту шифрованого повідомлення і відповідного йому відкритого тексту, повинне бути не менше загального числа можливих ключів;

число операцій, необхідних для розшифровування інформації шляхом перебору ключів, повинно мати чітку нижню оцінку і виходити за межі можливостей сучасних комп'ютерів (з урахуванням можливості використання мережевих обчислень);

знання алгоритму шифрування не повинне впливати на надійність захисту;

незначна зміна ключа повинна приводити до істотної зміни виду зашифрованого повідомлення навіть при використанні того самого ключа;

структурні елементи алгоритму шифрування повинні бути незмінними;

додаткові біти, що вводяться в повідомлення в процесі шифрування, повинні бути цілком і надійно сховані в шифрованому тексті;

довжина шифрованого тексту повинна бути рівна довжині вихідного тексту;

не повинно бути простих (які легко встановлюються) залежностей між ключами, що послідовно використовуються в процесі шифрування;

будь-який ключ з безлічі можливих повинен забезпечувати надійний захист інформації;

алгоритм повинен допускати як програмну, так і апаратну реалізацію, при цьому зміна довжини ключа не повинна призводити до якісного погіршення алгоритму шифрування.

До найбільш поширених способів захисту інформації на під`єднуючому носію, в призначеному для користувача середовищі, відносяться:

Створення прихованого розділу;

Створення архіву, заблокованого паролем;

Обмеження доступу до файлів / папок.

Перераховані способи захисту інформації мають ряд недоліків. Наявність прихованих розділів легко встановити, порівнюючи фактичну і реальну місткість носія інформації. Створення архівів заблокованих паролем, неминуче збільшує:

Імовірність відсутності програмного забезпечення на ПК;

Тимчасові витрати на створення-розпакування архіву;

Можливість введення неправильного (випадкового) пароля при створенні архіву;

Можливість часткової втрати інформації в процесі створення архіву, особливо зростаючої при використанні флеш-карт (через перевищення числа циклів запису-читання гарантованих виробником).

Обмеження доступу до файлів / папок здійснюється, як правило, за допомогою додаткового програмного забезпечення: Folder Crypto Password 3.1; Secure Folder 2.4; Hide Folder; Lock Folder XP і.т.д. або вбудованими засобами операційної системи (ОС). В цьому випадку, доступ до інформації, що захищається обмежується адміністративними засобами самої ОС, що само по собі є ненадійним.

У зв'язку з вищевикладеним, можна зробити висновок про те, що для надійного захисту даних користувачів, єдиним варіантом, є використання будь-якої криптозахисту в режимі реального часу. Це дозволить реалізувати безперервну роботу алгоритму шифрування / дешифрування трафіку від ПК до носія інформації в процесі запису / читання.

CyberSafe Top Secret - програма для захисту інформації, яка використовує сучасні алгоритми шифрування (RSA, AES, BlowFish та ін.). Наданий CyberSafe Top Secret набір інструментів і функцій, застосовується у всіх сферах роботи з інформацією: захист конфіденційної інформації, захист E-mail кореспонденції, створення і перевірка цифрових підписів. CyberSafe Top Secret підтримує шифрування на основі інфраструктури відкритих ключів (Public Key Infrastructure), дозволяє шифрувати розділи жорстких дисків комп'ютера, створювати віртуальні зашифровані диски будь-яких розмірів, а також приховувати логічні диски і зашифровані файли і папки на комп'ютері користувача.

CyberSafe надає можливість зашифрувати файли і папки різними способами. При захисті файлів на локальному комп'ютері, вони можуть бути розміщені на зашифрованому розділі логічного диска, збережені на віртуальний зашифрований тому, або зберігатися в папці, захищеної за допомогою функції прозорого шифрування.

При передачі файлів іншим користувачам може бути використана інфраструктура відкритих ключів, файли можуть бути зашифровані паролем або поміщені в зашифрований саморозпаковується.

У той час як інші програми зберігають приватні ключі користувачів, на своїх серверах, в CyberSafe ваш приватний ключ знаходиться тільки на нашому комп'ютері.

Інші програми для зберігання конфіденційних файлів використовують криптодиски, які також уразливі. У CyberSafe для захисту файлів використовується прозоре шифрування з системою довірених додатків, що забезпечує додатковий захист ваших файлів.

Висновок. Криптографія дуже консервативна. Нові засоби шифрування не зважають надійними доти, поки їх ретельно не розібрали "по кісточках" професійні криптоаналітики. Для цього їм повинен бути доступний вихідний код цих програм. Розробники комерційних програм цей код не публікують через побоювання, що конкуренти скористаються їхніми ідеями. Тому програми з закритим вихідним кодом не користуються довірою у фахівців. Небезпека застосування таких програм полягає в тому, що гіпотетично за закритим кодом розробниками може бути захований потайний "чорний хід" (backdoor) - можливість зламати шифр, навіть не знаючи пароля. Саме виходячи з цих міркувань набагато краще користуватися для цілей шифрування програмами з відкритим вихідним кодом.

Література

1. Хореев П.В. Методы и средства защиты информации в компьютерных системах – М.: Издательский центр «Академия». - 2005.
2. Соколов А.В., Степанюк О.М. Защита от компьютерного терроризма. Справочное пособие. – СПб.: БХВ – Петербург; Арлит 2002. – 496 с..
3. Мельников В.В. Защита информации в компьютерных системах. М.: Финансы и статистика. – 1997. – 364 с..

К.т.н., доцент Ільєнко А.В., Тригуб Д.А.
Національний авіаційний університет (НАУ),
Україна

ПРАКТИЧНІ ПІДХОДИ ВИКОРИСТАННЯ КРИПТОГРАФІЧНИХ АЛГОРИТМІВ СИМЕТРИЧНОГО ТА АСИМЕТРИЧНОГО ШИФРУВАННЯ ДЛЯ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ЕЛЕКТРОННИХ ПЛАТІЖНИХ СИСТЕМ

Вступ. Нині у всьому світі розвиток систем платежів характеризується поступовим звуженням сфери використання готівки та паперових платіжних документів, переходом до нових платіжних інструментів і сучасних платіжних технологій. Цифрові гроші широко залучаються до обігу і стають важливим інструментом фінансової інфраструктури економічно розвинутих країн.

Усі добре розвинуті країни намагаються максимально зменшити кількість операцій з готівками і готівкової маси в обігу. Для цього центральні банки та уряди застосовують цілий ряд заходів, одним з яких є розрахунки за допомогою платіжних систем з пластиковими картками (у свою чергу внутрішньодержавних, а також міжнародних).

Схожі процеси відбуваються й у банківській сфері України. Особливо важливу роль тут відіграє Національний банк України.НБУ бере безпосередню участь у розробці нових засобів плтатежів та організації електронного грошового обігу на території України.

Однак, як і кожна інформаційна система, дана СЕП потребує захисту.

Постановка задачі. Задачею даних досліджень є оцінка, порівняння та аналіз криптографічних алгоритмів симетричного та асиметричного шифрування даних задля забезпечення безпечного проведення електронних платежів та вибір найкращих із них.

Криптографічні методи захисту інформації систем електронних платежів

Система електронних платежів захищається у комплексі засобів та заходів, а саме: нормативно-правових, організаційних, апаратних, програмних та

адміністративних. Тільки за допомогою таких методів можна створити захищену СЕП.

Існує ще один ефективний метод захисту інформації СЕП – криптографічний. Використання криптографічного захисту інформації при побудові політики безпеки платіжної системи значно посилює безпеку роботи системи.

За принципами використання криптографічний захист може бути вбудованим у платіжну систему або бути додатковим механізмом, який може відключатися.

Інформацію щодо симетричних та асиметричних методах шифрування можна побачити нижче у порівняльних таблицях.

Таблиця 1

Порівняння симетричних алгоритмів шифрування

Назва	**Розмір блоку, біт**	**Розмір ключа, біт**	**Число раундів**	**Тип**	**Основні операції**	**Криптостійкість**	**Автор**
AES	128	128/192/256	10/12/14	Мережа замін-перестановок (SP)	SubBytes(),ShiftRows(), MixColumns(), AddRoundKey()	Достатньо надійний для захисту даних, які становлять державну таємницю	Вінсент Даймен
ГОСТ 28147-89	64	256	32/16	Мережа Фейстеля	Складання по модулю 2^{32}, перестановка, кільцева сума, циклічний здвиг	Стійкий до лінійного та диференціального криптоаналізу	КГБ, 8-е управління

Blowfish	64	від 32 до 448	16	Мережа Фейстеля	Складання по модулю 2^{32}, підстановка, кільцева сума	Криптостійкість налаштовується за рахунок зміни кількості раундів шифрування та S-блоків	Брюс Шнайєр
DES	64	56+8 перевірочних	16	Мережа Фейстеля	Підстановка, перестановка, кільцева сума	Достатньо надійний алгоритм	IBM
3DES	64	112 або 168	48	Мережа Фейстеля	Підстановка, перестановка, кільцева сума	Достатньо надійний алгоритм	IBM

Таблиця 2

Порівняння асиметричних алгоритмів шифрування

Назва	**Розмір відкритого ключа, біт**	**Розмір закритого ключа, біт**	**Криптостійкість**	**Автор**
RSA	512/1024/2048 /4096	512/1024/2048 /4096	2,7 × 10^{28} для ключа 1300 біт	Р. Рівест, Аді Шамір, Леонард Адлеман
DSA	160-256	1024-3072	Зловмисник отримує усі відкриті параметри підпису і якийсь набір пар (повідомлення, підпис) і намагається, використовуючи цей набір, створити дійсний підпис для нового повідомлення, що не представлений в наборі.	NIST
Elgamal	128	від 256	При однаковій довжині ключа криптостійкість дорівнює RSA, 2,7 × 10^{28} для ключа 1300 біт	Т. Ель-Гамаль
Diffie-Hellman	1024	1024	Протокол Діффі-Хеллмана відмінно протистоїть пасивному нападу, але в разі реалізації атаки «людина посередині» він не встоїть.	У. Діффі, М. Хеллман
ECDSA	64/128/160/224/256/384/512	64/128/160/224/256/384/512	Криптостійкість і швидкість роботи вище, ніж у RSA	NIST

Еліптична криптографія	150/205/234/512/768/1024/1280/1536/2048	64/128/160/224/256/384/512	Криптостійкість вище, ніж у RSA	Н. Коблиць, В.Міллер

Стандартно для побудови захисту СЕП використовують алгоритми 3DES (симетричний) та AES (асиметричний) як найбільш ефективні.

Наукова новизна. На основі проведеного аналізу та порівняння можна стверджувати, що ще одним ефективним криптографічним способом захисту СЕП буде використання алгоритмів AES 256 (як симетричний) та еліптичну криптографію (використання асиметричних алгоритмів). AES 256 являється більш надійним у порівнянні з 3DES (більші розміри ключів). А також у порівнянні з RSA при рівних рівнях захисту явна обчислювальна перевага належить саме криптографії на основі еліптичних кривих з коротшою довжиною ключа.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Брюс Шнайер. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на Си. – М.: Издательство ТРИУМФ, 2002.
2. Т. Кормен, Ч. Лейзерсон, Р. Ривест. Алгоритмы: построение и анализ. – М.: МЦНМО, 2002.
3. Забечников С. В. 3-31 Криптографические протоколы их применение финансовой коммерческой деятельности: Учебное пособие для вузов. - М.: Горячая линия-Телеком, 2007. - 320 с.
4. Гатчині Ю.А., Коробейников А.Г. Основи криптографічних алгоритмів. Навчальний посібник. - СПб.: СПбГІТМО (ТУ), 2002. - 29 с.

Тихий Н.С.
Національний авіаційний університет, Україна

ЗАХИСТ ІНФОРМАЦІЇ НА ОСНОВІ КРИПТОГРАФІЧНИХ ХЕШ-ФУНКЦІЙ

Вступ В останні роки першорядним фактором, що впливає на політичну і економічну складові національної безпеки, є ступінь захищеності інформації та інформаційного середовища. Ось чому важливе, значення набувають питання забезпечення безпеки (інформації та інформаційного середовища.) Інформаційних і телекомунікаційних технологій і гарантованого захисту даних в комп'ютерних мережах економічно значущих структур. Криптографічні методи знайшли широке застосування в практичній інформатиці для вирішення численних проблем інформаційної безпеки.

Актуальність Хеш-функції довгий час використовуються в комп'ютерних науках, є функціями, математичні чи інші, які отримують на вхід рядок змінної довжини (звану прообразом) і перетворюють її в рядок фіксованої, зазвичай менший, довжини (звану значенням хеш-функції) . Як просту хешфункцію можна розглядати функцію, яка отримує прообраз і повертає байт, що представляє собою XOR всіх вхідних байтів. Сенс хеш-функції полягає в отриманні характерної ознаки, прообразу-значення, за яким аналізуються різні прообрази при вирішенні оберненої задачі. Так як зазвичай хеш-функція являє собою співвідношення "багато до одного", неможливо з усією впевненістю сказати, що два рядки співпадають, але їх можна використовувати, отримуючи прийнятну оцінку точності.

Мета – реалізація забезпечення захисту інформації на основі криптографічних хеш-функції.

Викладення матеріалу Під терміном хеш-функція прийнято розуміти алгоритм перетворення деякого об`єму інформації в більш коротку послідовність символів за допомогою математичних методів. Практичну значимість хеш-функції можна простежити в самих різних областях. Так, їх можна задіяти при перевірці файлів і програм на предмет цілісності. Також криптографічні хеш-функції задіються в алгоритмах шифрування [1].

Використання хеш-функцій поширене при організації обміну документами, що містять електронно - цифровий підпис. Хешується в даному випадку підписується файл, для того щоб його одержувач міг упевнитися в тому, що він справжній. Хоча формально хеш-функція не входить в структуру електронного ключа, вона може фіксуватися у флеш-пам`яті апаратних засобів, за допомогою яких підписуються документи, таких як, наприклад, eToken.

Ще одна можлива сфера застосування хешування - організація алгоритмів перевірки паролів, встановлених для розмежування доступу до тих чи інших файлових ресурсів. На більшості серверів, доступ до яких підлягає розмежуванню, паролі зберігаються у вигляді хешірованних значень. Це цілком логічно - якби паролі були представлені в вихідному текстовому вигляді, хакери, отримали доступ до них, могли б запросто читати секретні дані. У свою чергу, на основі хеш обчислити пароль непросто [2].

У криптографічних додатках ключові функції хешування мають задовольняти наступні основні вимоги:

неможливість фабрикації;

неможливість модифікації.

Схема Рабіна базується на схемі Меркеля-Дамгарда. Функція стиснення замінюється будь-яким алгоритмом шифрування, у даному випадку алгоритмом AES. Входами функції стиснення являються блок повідомлення і вихід попереднього блоку. Вихід являється дайджестом повідомлення. Хеш-значенням всього повідомлення є вихід останнього блоку. Іншими словами дайджест повідомлення Мі дорівнює $H_i = E(M_i, H_{i-1})$ [3].

Хеш-значенням всього повідомлення являється вихід останнього блоку. Розмір дайджесту співпадає з розміром блочного шифру даних в основній криптографічній системі.

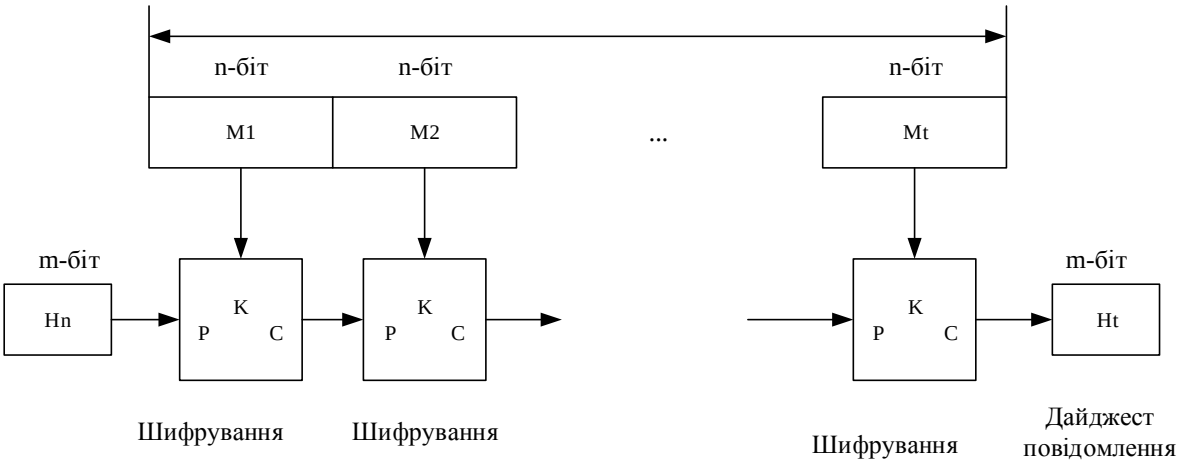


Рис. 1. Схема Рабіна

Висновки Було проаналізовано основи організації захисту в сучасних комп'ютерних системах та мережах, типи та алгоритмів формування хеш-функцій та на базі цих досліджень сформовано хеш-функцію на базі схеми Рабіна та алгоритму AES.

Література:

1. Основы криптографии : [учеб. пособ. 2-е изд., исп. и доп.] / [А. П. Алферов, А. Ю. Зубов, А. С. Кузьмин, А. В. Черемушкин]. — М : Гелиос АРВ, 2002. — 480 с.
2. Панасенко С.П., Алгоритмы шифрования. Специальный справочник. – СПб.: БХВ-Петербург, 2009, - 576 с.
3. Шнайер Б. Практическая криптография / Н. Фер- гюсон, Б. Шнайер. – М.: Вильямс, 2005. – 425 с

MATEMATIKA

Нечипоренко Н.О.
Запорізький національний технічний університет, Україна

ПРО ВІДНОВЛЕННЯ ФУНКЦІЇ, ЩО МАЄ ЗАДАНЕ ЧИСЛО ЕКСТРЕМУМІВ

Задача апроксимації табличних даних є однією з основних задач, що виникають при обробці результатів експериментів. У багатьох випадках у експериментатора є додаткова інформація про геометричні властивості відновлюваної функції, яку необхідно врахувати та зберегти.

Розглядається задача відновлення функції $f(x)$, що належить $K_m[a;b]$ – множині функцій, які мають на $[a;b]$ не більше ніж m внутрішніх екстремумів, за її наближеними значеннями f_j, $j=\overline{1,N}$ в вузлах x_j, $j=\overline{1,N}$ сітки $\Delta=\{a=x_1<x_2<...<x_N=b\}$.

Уточнимо поняття внутрішнього екстремуму. Нехай I – деякий інтервал відрізка $[a;b]$. Нехай також $\varphi(x)=C=const \quad \forall x\in I$ і існують такі $\alpha,\beta\in[a;b]\setminus I$ (причому $\alpha\le\min\limits_{x\in I}x$, $\beta\ge\max\limits_{x\in I}x$), що $\varphi(x)<C$ або $\varphi(x)>C$ $\forall x\in[\alpha;\beta]\setminus I$. Будемо говорити, що число внутрішніх екстремумів функції $\varphi(x)$ на $[a;b]$ дорівнює мінімальному на $[a;b]$ числу інтервалів з описаною вище властивістю.

В якості відновлювальної можна прийняти одну з наступних функцій:

а) функцію $S_m(x)$, яка є рішенням задачи

$$\delta(S_m)=\inf_{\varphi\in K_m[a;b]}\delta(\varphi),\quad \text{де}\quad \delta(\varphi)=\max_{1\le i\le N}|\varphi(x_i)-f_i|;$$

б) функцію $\overline{S_m}(x)$, яка має мінімальне число внутрішніх екстремумів на $[a;b]$ і задовольняє умові

$\max\limits_{1\le i\le N}\left|\overline{S_m}(x_i)-f_i\right|\le\varepsilon$, де ε – задане дійсне число.

Доведено, що розв'язок кожної з поставлених задач існує. Розроблені алгоритми побудови функцій $S_m(x)$ і $\overline{S_m}(x)$.

FYZIKA

Teoretická fyzika

Арынов Б.М.

Казахстан, г.Алматы, КазНПУ им. Абая

ПРОБЕГ ТЯЖЕЛЫХ ЗАРЯЖЕННЫХ ЧАСТИЦ

Полный путь, проходимый частицей с начальной энергией E_0 в веществе до того, как ее скорость не станет равной тепловой, определяется соотношением:

$$\overline{R_0}(E_0) = \int_{E_0}^{0} \frac{dE}{dE/dx} = \int_{0}^{E_0} \frac{dE}{-dE/dx}, \qquad (1)$$

где $\left(-\frac{dE}{dx}\right)$ – полные удельные потери энергии за счет всех механизмов взаимодействия – неупругого взаимодействия с атомами (ионизационные потери), упругого рассеяния в кулоновском поле ядра и в поле ядерных сил, упругого рассеяния в экранированном поле атома и, наконец, неупругих ядерных взаимодействий при больших энергиях частиц. Если ограничится областью энергий не выше ~100 МэВ, то вкладом неупругого ядерного взаимодействия в потери энергии можно пренебречь. Потери энергии за счет упругого рассеяния составляют малую долю от ионизационных потерь (~0,1%), за исключением области малых энергий для частиц с небольшими зарядами и массами.

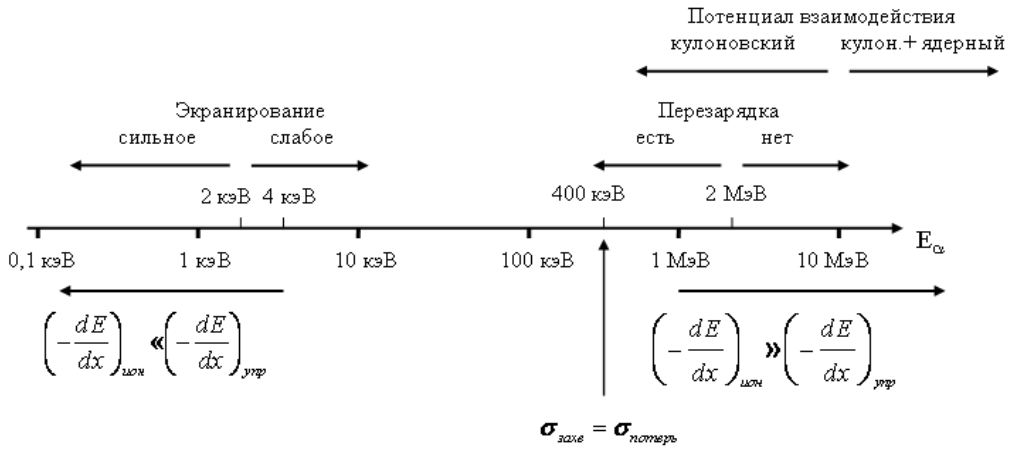


Рис.1. Области энергий для процессов взаимодействия α-частиц с Al

Поэтому если вычислять путь не до полной остановки частицы, а до некоторой энергии E_{min}, выше которой ионизационные потери преобладают над упругими, то

$$\overline{R_0}(E_0) = \int_{E_{\min}}^{E_0} \frac{dE}{(-dE/dx)_{ион}}, \qquad (2)$$

где для вычисления ионизационных потерь используется формула Бете – Блоха. В этом случаи среднее значение длины траектории:

$$\overline{R_0} \sim \frac{M}{q^2 \rho(Z/A)} f(V). \qquad (3)$$

Практически зависимость $\overline{R_0}(E_0)$ (соотношение «пробег-энергия») получают путем численного интегрирования формулы Бете – Блоха.

Из формулы (3) следует, что в данной среде отношение длин пробегов разных частиц с одинаковыми начальными и конечными скоростями определяется соотношением

$$\frac{R_{01}}{R_{02}} = \frac{M_1 q_2^2}{M_2 q_1^2} = \frac{E_1 q_2^2}{E_2 q_1^2}, \qquad (4)$$

т.к. при равных скоростях энергии пропорциональны массам частиц. Это позволяет по известной зависимости $\overline{R_0}(E_0)$ для одного сорта частиц получить аналогичную зависимость для другого сорта частиц в том же веществе. Например, нужно найти пробег в Al α-частиц с энергией 10 МэВ, пользуясь известной зависимостью «пробег-энергия» для протонов в Al:

$$\overline{R_{0\alpha}}(10\,МэВ) = \frac{1}{4}\frac{4}{1}\overline{R_{0p}}(E_p = \frac{1}{4}\cdot 10\,МэВ) = \overline{R_p}(2{,}5\,МэВ)$$

Единственное допущенное, сделанное при получении соотношения (4), состоит в том, что граничная энергия E_{min} принята одинаковой для частиц с разными зарядами. Этим допущением можно пользоваться, если речь идет о достаточно энергичных частицах, для которых весь пробег намного превышает ту его часть, где происходит перезарядка и изменение среднего ионизационного потенциала.

Пробеги частиц одного сорта и с одной начальной энергией несколько отличаются. Разброс величины пробегов около среднего значения обусловлен статистическим характером потерь энергии каждой частицей в отдельных актах

взаимодействия с электронами. На практике разброс длин пробегов измеряют по кривой пропускания, т.е. регистрируя число частиц, прошедших различную толщину вещества. Вид кривой пропускания для тяжелых заряженных частиц показан на рис. 2.

Толщина вещества, за которой поток частиц уменьшается вдвое, называется средним пробегом $R_{ср}$. Если измеренное распределение продифференцировать, то получим распределение пробегов P(R) вблизи среднего значения $R_{ср}$, которое достаточно хорошо описывается распределением Гаусса:

$$P(R)dR = \frac{1}{\left(2\pi\overline{\Delta R^2}\right)^{1/2}} \exp\left(-\frac{\left(R-R_{cp}\right)^2}{2\overline{\Delta R^2}}\right)\cdot dR, \qquad (5)$$

где $\overline{\Delta R^2} = \overline{\left(R-R_{cp}\right)^2}$ – дисперсия распределения P(R). Относительный разброс пробегов $(\overline{\Delta R^2})^{1/2} / R_{cp}$ носит название страгглинга.

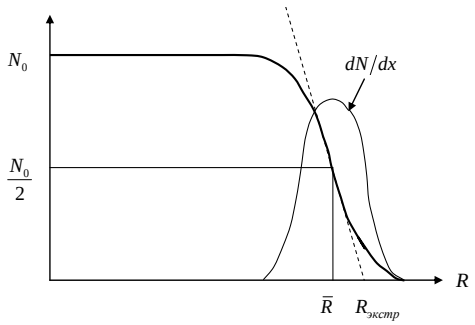
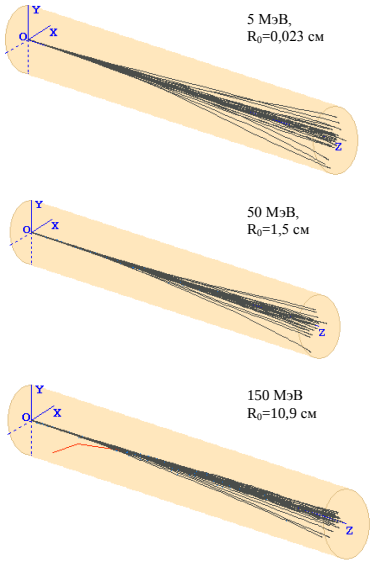


Рис.2. Кривая пропускания для α-частиц

Вычисленная по формуле (2) величина $\overline{R_0}$ и измеренная R_{cp} носят одинаковые названия «средний побег». В действительность они характеризуют разные величины: $\overline{R_0}$ – это средняя длина траектории частиц в веществе, $R_{ср}$ – это среднее значение толщины вещества, до которой доходят частицы. Поскольку траектории частиц из-за многократного рассеяния не является строгой прямой линией, то всегда $\overline{R_0} > \overline{R_{cp}}$. Измеряемый на практике пробег является проекцией траектории частиц на первоначальное направление их движения. Поэтому измеряемый разброс пробегов обусловлен не только флуктуациями потерь энергии, но и разбросом длин проекций одинаковых по длине траекторий. Для тяжелых заряженных частиц разница между R_0 и $R_{ср}$ невелика. На рис. 3,4 показаны траектории протонов в легком (Be) и тяжелом

(Pb) веществах, рассчитанные методом Монте-Карло по программе **КЛ**. Для каждого значения энергии частиц рассчитано по 30 траекторий. На всех рисунках показанная толщина поглотителя равна рассчитанной по формуле (2) средней длине траектории частиц $\overline{R_0}$ при данной энергии.

Более наглядно степень различия между длиной траектории R_0 и пробегом R представлена на рис. 10, где показаны проекции траекторий рис.3 на плоскость (ZY). Значение координаты Z, где число частиц



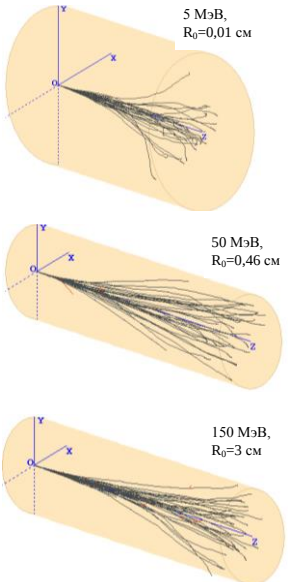


Рис.3. Траектории протонов в бериллии Рис.4. Траектории протонов в свинце

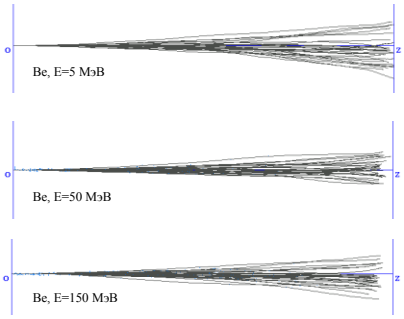


Рис.5. Проекции траекторий протонов в бериллии на плоскость (ZY)

вдвое меньше начального, это средний пробег в веществе частиц, имеющих среднюю длину траектории $\overline{R_0}$, которая на рисунках равна длине оси Z. Для более наглядной демонстрации влияния упругого рассеяния на характер траектории частиц масштаб по оси Y на рис. 5 увеличен вдвое.

На практике для определения энергии частиц по пробегу чаще используют на средний, а экстраполированный пробег, который меньше зависит от условий измерения. Экстраполированный пробег определяется точкой пересечения с осью абсцисс касательной, проведенной к кривой пропускания в точке ее максимального наклона (на рис.3 пунктирная линия). Например, для определения энергии α-частиц по их экстраполированному пробегу в воздухе $R^{\alpha}_{\text{экстр}}$ можно использовать эмпирическую формулу

$$R^{\alpha}_{экстр} \approx 0,31E^{3/2} \text{ см}; \quad 4<E<7 \text{ МэВ}. \qquad (6)$$

Для веществ с массовым числом А справедливо приближенное соотношение:

$$R^{\alpha}_{экстр} = 0,56R^{\alpha}_{экстр\ возд.}(см)\cdot A^{1/3} \ \ мг/см^2, \qquad (7)$$

где $R^{\alpha}_{экстр\ возд.}(см)$ – экстраполированный пробег α-частиц той же энергии в воздухе в сантиметрах. Экстраполированный пробег протонов в воздухе:

$$R^{p}_{экстр}(E) = R^{\alpha}_{экстр}(4E) - 0,2\,см; \qquad E > 0,5МэВ. \qquad (8)$$

Поскольку массовые тормозные способности в $МэВ/г\cdot см^{-2}$ для разных веществ близки, и пробеги в $г/см^2$ в разных веществах отличаются сравнительно мало.

Отметим основные закономерности, касающиеся разброса пробегов тяжелых частиц.

Разброс пробегов медленно уменьшается с увеличением энергии вплоть до $E/mc^2 \sim 2,5$ (до области минимума потерь), затем медленно растет. Так для протонов, тормозящихся в алюминии, имеем:

E_p, МэВ	2	20	200	2000	20000
Страгглинг, %	2	1,5	1,1	0,9	1,3

1. Страгглинг медленно растет с увеличением Z тормозящей среды при прочих равных условиях. Для протонов энергией 20 МэВ имеем:

Вещество	Be	Al	Cu	Pb
Страгглинг, %	1,3	1,5	1,6	1,8

2. Для частиц различных сортов, но имеющих одинаковые начальные скорости, величины страгглингов в данном веществе связаны соотношением:

$$\frac{\overline{\left(\Delta R_2^2\right)}^{1/2}}{R_{2cp}} = \left(\frac{M_1}{M_2}\right)\frac{\overline{(\Delta R_1^2)}^{1/2}}{R_{1cp}},$$

т.е. более тяжелая частица имеет меньший разброс пробегов (независимо от заряда). Например, разброс пробегов α-частиц с энергией 40 МэВ в 2 раза меньше, чем протонов с энергией 10 МэВ (их начальные скорости равны).

Литература

1. К.Н. Мухин. Экспериментальная ядерная физика. – М.: Энергоатомиздат, 1983.
2. Ю.М. Широков, Н.П. Юдин. Ядерная физика. – М.: Наука, 1972.
3. А.И. Абрамов, Ю.А. Казанский, Е.С. Матусевич. Основы экспериментальных методов ядерной физики: Учебное пособие для ВУЗов. – М.: Энергоатомиздат, 1985.

Solid state physics

Кучер В.А.
Національний технічний університет України "Київський політехнічний інститут імені І. Сікорського"

ФЕРОМАГНІТНІ ПЛІВКИ З ПЕРІОДИЧНИМИ СТРУКТУРАМИ З МАГНОННОЮ ЗАБОРОНЕНОЮ ЗОНОЮ – МАГНОННІ КРИСТАЛИ

Дослідження в галузі фізики фотонних кристалів стимулювали створення кристалів, які працюють в діапазоні частот видимого світла, на основі синтетичних опалів, колоїдних частинок, плівок з наноструктурами та ін. Властивості фотонних кристалів, зокрема, існування фотонної забороненої зони, залежать від довжини хвилі світла, що розповсюджується. Мініатюрні пристрої на основі фотонних кристалів можуть бути створені тільки для кристалів з довжиною хвилі видимого або інфрачервоного діапазонів спектру. Фотонні кристали із забороненою зоною в області радіочастот мають досить великі розміри, оскільки довжина хвилі електромагнітних хвиль в цьому діапазоні порядку декількох сантиметрів. Поряд з створенням фотонних кристалів з'явилася ідея створення і аналогічних кристалів, в яких розповсюджуючими хвилями є магнони (спінові хвилі).У таких кристалах відповідні властивості фотонних кристалів притаманні спіновим хвилям. Створення кристалів, подібних фотонним, на основі магнітних матеріалів (а саме, магнонних кристалів), в яких можуть розповсюджуватися спінові хвилі, має ряд переваг в порівнянні з фотонними кристалами. По-перше, довжина спінової хвилі, а відповідно, і властивості таких кристалів залежать від зовнішнього магнітного поля і можуть управлятися цим полем. По-друге, для широкого класу феромагнітних матеріалів в мікрохвильовому (радіочастотний) діапазоні довжина спінових хвиль, що розповсюджуються, порядку десятків або сотень мікрон. Таким чином, можна створити кристали з фотонної (або магнонної) забороненою зоною з розмірами порядку декількох міліметрів. Причому такі кристали можуть бути створені в пленарній геометрії, що може бути надзвичайно важливим для створення інтегральних пристроїв, зокрема, вузько

частотних оптичних або СВЧ фільтрів і високошвидкісних перемикачів. Необхідно відзначити, властивості магнонних кристалів вивчені ще дуже мало. Перші роботи, присвячені кристалів з магнонною забороненою зоною, фактично позначили проблему існування таких кристалів. Однак створення таких кристалів є надзвичайно перспективним і важливим як з наукової, так і з практичної точок зору. Зокрема, є проблема управління магнонною забороненою зоною з допомогою зовнішнього магнітного поля в одно- і двомірних магнонних кристалах. За рахунок спеціального підбору магнітних матеріалів в періодичній структурі можливе створення невзаємних магнонних кристалів з односторонньою прозорістю (тобто пропускаючих спінову хвилю тольки в одному напрямку і не пропускаючих в протилежному напрямку). Є також проблема поширення і дифракції світла в лінійному і нелінійному магніто-фотонних кристалах, зокрема, збільшення сумарного ефекту Фарадея за рахунок резонансного відображення хвиль і анізотропного перетворення хвилеводних мод в магніто-фотонних кристалах.

Розглянемо можливості створення магнонних кристалів, наведемо результати експериментальної реалізації таких кристалів, а також перспективи їх застосування.

Найпростіший одновимірний магнонний кристал - це строго періодична багатошарова структура, що складається з магнітних шарів з різною намагніченістю або така ж структура, але яка складається з магнітних і немагнітних шарів. Реалізувати таку структуру досить складно, оскільки при зростанні шарів може легко порушитися періодичність їх магнітних властивостей, що призведе до руйнування структури магнонного кристала, що володіє магнною забороненою зоною. Кращим з точки зору застосувань є двомірний магнонний кристал, виготовлений на основі феромагнітних плівок. Такий кристал фактично представляє собою феромагнітний хвилевід з двовимірними неоднорідностями намагніченості в ньому. Такою неоднорідністю може бути, наприклад, імплантовані елементи іншого феромагнетика або отвори. Розглянемо створення магнонного кристала за допомогою феромагнітних плівок залізо-ітрієві граната (ЗІГ), вирощена епітаксійно на немагнітній підкладці з галій-гадолінієвого граната. Магнітостатичні спінові хвилі (МСХ) легко збуджуються в таких плівках за допомогою мікросмужкових перетворювачів. Через високу якість плівок втрати на поширення МСХ в них не дуже великі, тому МСХ можуть в них

поширюватися без істотного загасання на відстані, рівним багатьом довжинам хвиль. Отже, розглянута структура являє собою плівку ЗІГ з отворами. Діаметр отворів і їх періодичність вибиралися близькими до половини довжини хвилі (для того щоб виконувалася умова брегівского відображення).

Спектр спінових хвиль в феромагнітній плівці з двовимірними періодичними структурами знаходиться з рішень рівнянь Ландау-Ліфшиця для руху намагніченості і рівнянь Максвелла з відповідними граничними (па поверхні плівки) і періодичними умовами. У результаті рішення граничної задачі виходить загальне дисперсійне рівняння:

$$cosk_1 dcosk_2 d + \left(\frac{k_1}{2k_2} + \frac{k_2}{2k_1}\right) sin\, k_1 d sin\, k_2 d = \cosh(2q_z D)$$

де d товщина плівки, D - період періодичної структури, q_z - хвильове число спінової хвилі,що розповсюджується, k_1 і k_2 – константи розповсюдження спінових хвиль, що визначаються наступними співвідношеннями:

$$k_1 = \sqrt{q_z^2 - k_0^2 \mu_\perp},\ k_2 = \sqrt{q_z^2 - k_0^2 \varepsilon},$$

$$\mu_\perp = \frac{(\mu^2 - v^2)}{\mu},\ \mu = 1 + \frac{\omega_H \omega_M}{\omega_H^2 - \omega^2},\ v = \frac{\omega_H \omega_M}{\omega_H^2 - \omega^2},$$

$$\omega_H = \gamma H,\ \omega_M = 4\pi\gamma M_0,$$

де H - зовнішнє магнітне поле, M_0 - намагніченість насичення феромагнетика, ω - частота спінової хвилі. Спектр хвиль в періодичній структурі представлений на рис.3.

Видно, що в спектрі з'являються заборонені зони, які відповідають частотам при яких поширення хвилі в періодичній структурі стає неможливим. Важливо відзначити, що положення забороненої зони в частотному спектрі залежить від параметрів плівки (періодичної структури), а також від зовнішнього магнітного поля. Таким чином, змінюючи магнітне поле, можна управляти спектром хвиль, що розповсюджуються, в магнітному фотонному кристалі.

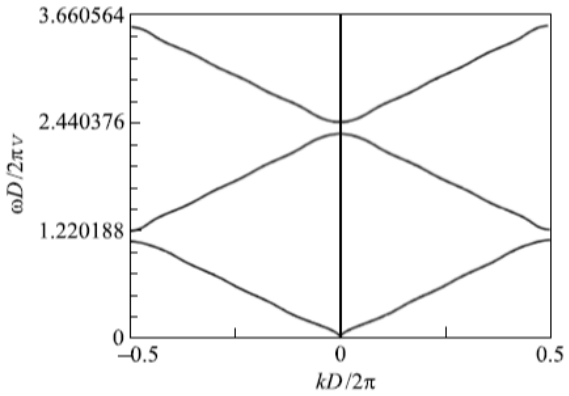


Рис.3 Спектр могнітостатичних спінових хвиль в періодичній структурі (період структури *D =10 мк, v* – групова швидкість спінової хвилі)

Література:

1. K.Sakoda, *Optical Properties of Photonic Crystals*, Springer Series in Optical Sciences, Springer Verlag 2001.
2. S.G. Jonson and J.D. Joannopoulos, *Photonic Crystals: The Road from Theory to Practice*, Kluwer, Boston, 2002
3. http://www.jetpletters.ac.ru/ps/33/article_467.pdf

STAVEBNICTVÍ A ARCHITEKTURA

Moderní technologie výstavby, rekonstrukce a restaurování

Ербол Б.Е.,Турсумбекова Х.С.

РЕКОМЕНДАЦИИ ДЛЯ ОПРЕДЕЛЕНИЯ ОБЩЕГО МОДУЛЯ УПРУГОСТИ ДВУХСЛОЙНОЙ СИСТЕМЫ

Научной работе мы представили два варианта расчета конструкций дорожной одежды на сопротивление по упругому прогибу.

Первый вариант, действующий на РК, послойный расчет дорожной одежды выполняли с использованием номограммы, которая связывает пять параметров двухслойной системы. В которым основным принципом является проведение вертикаль из точки на горизонтальной оси, соответствующей значению h/D, и горизонтальная прямая из точки на вертикальной оси, соответствующей отношению E_2/E_1. Точка пересечения этих прямых дает искомое значение $E_{общ}/E_1$. Зная величину E_i вычислить $E_{общ}$. Данный метод расчета дает не точный значения $E_{общ}/E_1$ так как каждый человек по каждому попадает на точку отношение E_2/E_1 с значению h/D.

Второй вариант расчета дорожной одежды на сопротивление по упругому прогибу рассчитывается с помощью разработанной алгоритма для определения $E_{общ}/E_1$ с помощью расчетных таблиц.

При расчете нам необходимо вычислит общий модуль упругости на границе слоев E′общ, Мпа для каждого слоя по формуле: (7.3). Независимо от результата расчета, полученного по расчету, общий модуль упругости должен быть не менее указанного в Таблице 7.1

Минимальные значения общего модуля упругости [1]

Таблица 7.1

Категория дороги	**Минимальный требуемый модуль упругости дорожной одежды, МПа**		
	Капитального типа	**Облегченного типа**	**Переходного типа**
I	230	-	-
II	220	-	-
III	180	160	-
IV	-	130	90
V	-	100	80

Общий модуль упругости дорожной одежды, рассчитанный для нагрузки группы А2, независимо от результатов расчета, должен быть не менее 230 МПаДля дорожных одежд, рассчитанных на осевую нагрузку группы А2, следует предусматривать двухслойное асфальтобетонное покрытие общей толщиной не менее 15 см на основании, укрепленном органическими вяжущими, и не менее 15 см на основании, укрепленном неорганическими вяжущими. Обязательным является как минимум двухслойное основание. Верхний слой основания должен быть укреплен органическими, либо неорганическими или бесцементными вяжущими (золы уноса, шлаки и т.п.). При этом толщина верхнего слоя основания, укрепленного вяжущим материалом, независимо от результатов расчета должна быть не менее:

12 см – слои, укрепленные органическими вяжущими;

20 см – слои, укрепленные неорганическими вяжущими, в т.ч. зольными, шлаковыми и бокситовыми вяжущими.

Исходя из условия прочности по формуле 7.1 дорожную одежду конструируют таким образом, чтобы на ее поверхности был обеспечен общий модуль упругости, равный расчетному:

$$Eобщ = E_{p} = E_{mp} \times E_{p} \qquad (7.1)$$

$$Eобщ = \text{Еобщ/Е1} \times Ec \qquad (7.2)$$

$E_{общ}/E_1$ определяем по формуле (7.3)

$$Eобщ/E1 = \left[\frac{F-K}{50} \times \left(\frac{E_{общ}}{E_1} - Va \right) \times 1000 \right] + K, \qquad (7.3)$$

где: F – значения в зависимости отношения h/D к Va, вычисляем по формуле: (7.4)

K – Значения в зависимости от h/D к Vb, который вычисляем по формуле: (7.5)

Отношение E_2/E_1, где E_1 – модуль упругости материала верхнего слоя, Мпа; E2, – модуль упругости на поверхности нижнего слоя, Мпа

Va- Значения по таблице в меньшую сторону зависимости от значения отношение E_2/E_1

$$F = \left[\frac{Fb-Fa}{100} \times \left(\frac{h}{D} - Wa \right) \times 1000 \right] + Fa, \qquad (7.4)$$

где: Fb – значения в зависимости отношения Wb к Va, который определяем по таблице :

Fa – значения в зависимости отношения Wa к Va, который определяем по таблице

отношение h/D где: h – толщина верхнего слоя, см; D – расчетный диаметр круга отпечатка сдвоенных колес расчетного автомобиля, см;

Wa- Значения по таблице в меньшую сторону зависимости от значения отношение h/D

$$K = \left[\frac{Kb-Ka}{100} \times \left(\frac{h}{D} - Wa \right) \times 1000 \right] + Ka, \qquad (7.5)$$

где: Kb – значения в зависимости отношения Wb к Vb, который определяем по таблице 7.4 :

Ka – значения в зависимости отношения Wa к Vb, который определяем по таблице 7.4

отношение h/D где: h – толщина верхнего слоя, см; D – расчетный диаметр круга отпечатка сдвоенных колес расчетного автомобиля, см;

Wb- Значения по таблице в большую сторону зависимости от значения отношение h/D

Посоленный расчет дорожной одежды выполняем с использованием расчетных таблиц, которая связывает пять параметров двухслойной системы Таблица -7.1: отношение E_2/E_1; отношение h/D и отношение $E_{общ}/E_1$, где E_1 –

модуль упругости материала верхнего слоя, Мпа; E_2 – модуль упругости на поверхности нижнего слоя, Мпа; h – толщина верхнего слоя, см; D – расчетный диаметр круга отпечатка сдвоенных колес расчетного автомобиля, см; $E_{общ}$ – общий модуль упругости на поверхности верхнего слоя, Мпа. Зная значения любых четырех параметров, рекомендуется определить пятый по формуле (7.1)

Расчетные значения модулей упругости материалов следует назначать в соответствии с указаниями Приложения Б. [1] Значения модуля упругости материалов, содержащих органическое вяжущее, следует принимать при температуре +10°С во всех дорожно-климатических зонах. Так как конструкции дорожных одежд на перегонных участках подвергаются в основном воздействию подвижных нагрузок, а на стоянках, остановках, перекрёстках и т.п. - статическому воздействию от транспортных средств, значения модуля упругости асфальтового бетона в Приложении Б в Таблице Б.3 [2] даны применительно к этому виду режима нагружения конструкций.

Расчетные значения модулей упругости грунтов земляного полотна следует назначать в соответствии с указаниями Приложения В. [1]

Список литературы.

1. Проектирование дорожных одежд нежесткого типа. СН РК 3.03-19-2006* Издание официальное. Комитет по делам строительства Министерства индустрии и торговли РК Астана, 2007.
2. П.И. Теляев, инж. В.А. Мазуров, канд. техн. наук А.Е. Мерзликин, инженеры Е.И. Масленкова, Г.А. Муромова, И.Н. Налобин, Т.Е. Полтаранова. Методические рекомендации по автоматизации расчетов дорожных одежд нежесткого типа.
3. О.А Красиков. Оценка прочности расчет усиления нежестких дорожных одежд.

Zemleustroitelstvo

Бугаєнко О. А.
Київський національний університет будівництва і архітектури, Україна

АЛГОРИТМ ПЕРЕРОЗПОДІЛУ ЗЕМЕЛЬ ПРИ КОНСОЛІДАЦІЇ ЗЕМЕЛЬ В УКРАЇНІ

В умовах фрагментації сільськогосподарських земель в Україні зростає необхідність вдосконалення просторових параметрів окремих земельних ділянок в системі існуючих землеволодінь і землекористувань. Нині відповідні заходи характеризуються низькою ефективністю, однією із причин чого є відсутність ефективних механізмів перерозподілу земель, як основної складової консолідації земель.

Пропонується вдосконалення перерозподілу на основі вимог щодо рівноцінності перерозподілених земельних ділянок сільськогосподарського призначення за сукупністю якісних, просторово-технологічних та правових характеристик [1]. З метою досягнення рівноцінності перерозподілених земельних ділянок пропонується враховувати якість ґрунту відповідно до показників, які впливають на родючість ґрунтів щодо певних сільськогосподарських культур, виду сільськогосподарських угідь, наявності земельних поліпшень, конфігурації земельних ділянок, рельєфу, гідрографічних умов, місця розташування земельних ділянок, наявності обмежень та обтяжень у використанні [2]. Розрахунки здійснюються відповідно до методики [3].

Процес перерозподілу земель пропонується виконувати в наступному порядку:

Визначення земельних ділянок, які підлягають перерозподілу, відповідно до цілей, визначених проектом консолідації земель. Консолідація земель, як правило, має на меті зростання ефективності господарської діяльності, оновлення населених пунктів, розміщення інфраструктурних, соціально спрямованих об'єктів, здійснення природоохоронних заходів тощо [4, 5]. Відповідно, перерозподіл земель у складі консолідації земель спрямований на

формування землеволодінь і землекористувань таким чином, щоб їх розміри, межі та місце розташування відповідали встановленим завданням.

На першому етапі уточнюються земельні ділянки, які можуть бути залучені до перерозподілу та встановлюються характеристики, необхідні для зіставлення відповідно до вимог рівноцінності.

Створення основи перерозподілу земель. Реалізується шляхом поділу проектної території на блоки. Блок – це частина проектної території з однаковим типом землекористування, відмежована існуючими або запроектованими дорогами, іншими штучними або природними об’єктами [6]. У процесі формування блоків враховуються вид угідь, рельєф, гідрографічні умови, наявність обмежень та обтяжень у використанні.

Проектування блоків має відповідати цілям консолідації земель та здійснюється наступним чином:

а) межі блоків проектуються по межах існуючих земельних масивів. Таким чином створюється основа перерозподілу у випадку покращення параметрів земельних ділянок в межах масиву сільськогосподарських земель або його частини: усунення черезсмужжя земельних ділянок, зменшення відстаней між земельними ділянками в межах землекористування, покращення конфігурації земельних ділянок, зокрема, вирівнювання меж, розміщення меж відповідно до протиерозійних вимог щодо організації території, забезпечення під’їзду тощо;

б) проектування блоків без врахування меж існуючих земельних масивів – передбачає покращення параметрів земельних ділянок із зміною параметрів земельних масивів (оптимізація дорожньої мережі, забезпечення під’їзними шляхами, покращення конфігурації тощо);

3) розміщення в існуючій системі землеволодінь і землекористувань природоохоронних або інфраструктурних об'єктів, земельні ділянки яких мають встановлені параметри і обумовлюють зміну параметрів існуючих земельних земельних масивів.

Власне перерозподіл земельних ділянок.

Визначення параметрів перерозподілених земельних ділянок здійснюється із застосуванням евристичного або оптимізаційного підходу (їх

поєднання), заснованого на лінійному програмуванні. Земельні ділянки проектуються в межах блоків.

Встановлення меж земельних ділянок в натурі (на місцевості).

Правові аспекти формування земельних ділянок в процесі перерозподілу регулюються чинним законодавством. Залежно від вихідних умов, відповідно до законодавчих вимог щодо здійснення міни, купівлі-продажу, оренди, суборенди земельних ділянок.

Література:

1. Бугаєнко О. А. Оптимізація перерозподілу земель при впорядкуванні існуючих землеволодінь і землекористувань / О. А. Бугаєнко // Інженерна геодезія – 2016. – № 63. – С.99-109.
2. Бугаєнко О. А. Дослідження факторів, що впливають на проведення рівноцінного обміну земельних ділянок сільськогосподарського призначення / О. А. Бугаєнко // Містобудування та територіальне планування. – 2015. – № 57. – С.48-54.
3. Чибіряков В. К. Вдосконалення методики розрахунку рівноцінних земельних ділянок сільськогосподарського призначення при проведенні обміну / В. К. Чибіряков, М. А. Малашевський, О. А. Бугаєнко // Інженерна геодезія – 2015. – №62. – С. 85-94.
4. Hendricks A. Land consolidation for large-scale infrastructure projects in Germany /A. Hendricks, A. Lisec // Geodetski vestnik . 2013. - № 58(1). – P. 46-68.
5. FAO. The design of land consolidation pilot projects in Central and Eastern Europe [Електронний ресурс] / FAO. – Роме, 2003. – Режим доступу: http://www.fao.org/docrep/006/Y4954E/y4954e00.htm. – Назва з екрана.
6. Demetriou D. Land consolidation in Cyprus: Why is an integrated planning and decision support system required? / D. Demetriou, J. Stillwell, L. See // Land Use Policy. – 2012. - №29 (1). – P. 131-142.

CONTENTS

MODERNÍCH INFORMAČNÍCH TECHNOLOGIÍ

Computer engineering

Нукусова Б.К. ИНФОРМАТИКА ПӘНІ БОЙЫНША КРИТЕРИАЛДЫҚ БАҒАЛАУДЫ ЖОСПАРЛАУ ЖӘНЕ ҰЙЫМДАСТЫРУ **3**
Стовбчатий М. М. ВСТАНОВЛЕННЯ АВТОРСТВА ТЕКСТУ ЗА ДОПОМОГОЮ ДЕРЕВ ЗАЛЕЖНОСТЕЙ **6**
Мадеш Ж.М. РАЗРАБОТКА МЕТОДИКИ И АЛГОРИТМА ПОИСКА И ЛОКАЛИЗАЦИИ НЕИСПРАВНОСТЕЙ В СЕТЯХ ТИПА АТМ **10**

Počítače a programování

Пархоменко І.І., Носенко Ю.В. ЗАХИСТ WEB - ДОДАТКІВ В МЕРЕЖІ ІНТЕРНЕТ..... **17**

Software

Айдосов А., Заурбеков Н.С., Заурбекова Г.Н., Кзылбаев М.С., Аппакова А.А. МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ ДИНАМИКИ ВЕРТИКАЛЬНЫХ ДВИЖЕНИЙ В ОБЛАЧНОЙ АТМОСФЕРЕ ДЛЯ ОЦЕНКИ КАЧЕСТВА ВЕРТИКАЛЬНЫХ ДВИЖЕНИИ И ЧИСТОТЫ АТМОСФЕРНОГО ВОЗДУХА **21**
Пархоменко І.І.,Чигринюк В.Ю. ЗАХИСТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА **26**

Informační bezpečnost

Мелешко О.О., Голишевська І.В. СПОСОБИ ВИЯВЛЕННЯ ТА ЗАХИСТУ ВІД ШКІДЛИВИХ ПРОГРАМ **29**
Радик Т.В., Ільєнко А.В. ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ІНФОРМАЦІЇ З ВИКОРИСТАННЯМ ПОНЯТТЯ «ЦИФРОВОГО КОНВЕРТУ»..... **32**
Горобець В. О, Ильєнко А. В. ПРОГРАМНІ АСПЕКТИ ЗАХИСТУ НОСІЇВ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ НА ОСНОВІ КРИПТОГРАФІЧНИХ ПЕРЕТВОРЕНЬ **35**
Ільєнко А.В., Тригуб Д.А. ПРАКТИЧНІ ПІДХОДИ ВИКОРИСТАННЯ КРИПТОГРАФІЧНИХ АЛГОРИТМІВ СИМЕТРИЧНОГО ТА АСИМЕТРИЧНОГО ШИФРУВАННЯ ДЛЯ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ЕЛЕКТРОННИХ ПЛАТІЖНИХ СИСТЕМ..... **40**
Тихий Н.С. ЗАХИСТ ІНФОРМАЦІЇ НА ОСНОВІ КРИПТОГРАФІЧНИХ ХЕШ-ФУНКЦІЙ **45**

MATEMATIKA

Нечипоренко Н.О. ПРО ВІДНОВЛЕННЯ ФУНКЦІЇ, ЩО МАЄ ЗАДАНЕ ЧИСЛО ЕКСТРЕМУМІВ **48**

FYZIKA

Teoretická fyzika

Арынов Б. М. ПРОБЕГ ТЯЖЕЛЫХ ЗАРЯЖЕННЫХ ЧАСТИЦ **50**

Solid state physics

Кучер В.А. ФЕРОМАГНІТНІ ПЛІВКИ З ПЕРІОДИЧНИМИ СТРУКТУРАМИ З МАГНОННОЮ ЗАБОРОНЕНОЮ ЗОНОЮ – МАГНОННІ КРИСТАЛИ **56**

STAVEBNICTVÍ A ARCHITEKTURA

Moderní technologie výstavby, rekonstrukce a restaurování

Ербол Б.Е. РЕКОМЕНДАЦИЙ ДЛЯ ОПРЕДЕЛЕНИЯ ОБЩЕГО МОДУЛЯ УПРУГОСТИ ДВУХСЛОЙНОЙ СИСТЕМЫ **60**

Zemleustroitelstvo

Бугаєнко О.А. АЛГОРИТМ ПЕРЕРОЗПОДІЛУ ЗЕМЕЛЬ ПРИ КОНСОЛІДАЦІЇ ЗЕМЕЛЬ В УКРАЇНІ **64**

CONTENTS **67**

238931
239136
239166
239076
238701
239092
238875
239012
239022
239025
239106
238960
238061
239067
239188
239058