ISSN 2074-9481

Державна служба спеціального зв'язку та захисту інформації України
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»

ПРАВОВЕ, НОРМАТИВНЕ ТА МЕТРОЛОГІЧНЕ ЗАБЕЗПЕЧЕННЯ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ В УКРАЇНІ

Науково-технічний збірник

Засновник та видавець: Національний технічний університет України «КПІ»

Збірник випускається 2 рази на рік

Місце заснування: м. Київ, НТУУ «КПІ»

Випуск 1 (33) 2017

Заснований у 2000 р.

Київ 2017

УДК 681.3.067:34(477)(063)

Випуск 1 (33) періодичного науково-технічного збірника присвячено розгляду актуальних питань технічного захисту інформації. Розглядаються загальні питання інформаційних технологій і практичні аспекти захисту інформаційних ресурсів, нормативно-правові, методологічні і метрологічні аспекти захисту інформації в інформаційно-телекомунікаційних системах, захисту мовної інформації на об'єктах інформаційної діяльності, кібербезпека і захист критичної інформаційної інфраструктури, актуальні питання функціонування системи криптографічного захисту інформації, сучасні проблеми і тенденції розвитку системи захисту інформації.

Для науковців, аспірантів, інженерів, магістрів, спеціалістів, бакалаврів, студентів.

Збірник включено до переліку фахових видань (постанова ВАК України від 10.03.2010 р. № 1-05/2). Заснований згідно з рішенням Вченої Ради НТУУ «КПІ», протокол № 4 від 03.04.2000 р.

Відповідальний за випуск: Прокофьєв М. І., директор НДЦ «ТЕЗІС»

Над випуском працював редактор: Кулій Р. О.

Адреса редакції та видавця:
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Науково-дослідний центр «ТЕЗІС»
03056, Україна, м. Київ, проспект Перемоги, 37
(вул. Політехнічна, 12), корп. 17, оф. 406
тел. (044) 204-86-25, тел./факс (044) 204-83-85. Email: pnzzi@tesis.kiev.ua

Наукометричні бази: *Ulrichweb Global Serials Directory, Наукова періодика України, Base, OJS, EZB, ELAKPI, Національна бібліотека України імені В. І. Вернадського, Інститут проблем реєстрації інформації*

Збірник зареєстровано у Державному комітеті інформаційної політики, телебачення та радіомовлення України. Свідоцтво КВ № 5185 від 12.06.2001р.

Свідоцтво про внесення НТУУ «КПІ» до Державного реєстру видавців, виготівників і розповсюджувачів видавничої продукції № 211 серія ДК.

Видано за рішенням Вченої Ради КПІ ім. Ігоря Сікорського. Підписано до друку 14.07.2017р.
Наклад 100 прим. Формат 60x84/8. Облік.-видавн. арк. 18,7. Замовлення № 07-2 від 17.07.2017р.

ISSN 2074-9481

State Service for Special Communications and information security of Ukraine
National Technical University of Ukraine
«Igor Sikorsky Kyiv Polytechnic Institute»

LEGAL, REGULATORY AND METROLOGICAL SUPPORT OF INFORMATION SECURITY SYSTEM IN UKRAINE

Scientific and technical journal

Founder and publisher: National Technical University of Ukraine «KPI»

Journal produced 2 times a year

Place of foundation: Kyiv, NTUU «KPI»

Edition 1 (33) 2017

Established in 2000

Kyiv 2017

UDK 681.3.067:34(477)(063)

Edition 1 (33) periodical scientific and technical collection devoted to consideration of current issues of technical protection of information. The general issue of information technology and the practical aspects of protecting information resources, legal, methodological and metrological aspects of information security in the information and telecommunicational systems and the protection of linguistic information at the facilities of information activities, cyber security and critical information infrastructure protection, FAQs functioning of cryptographic security, current issues and development trends information security system.

For researchers, graduate students, engineers, masters, specialists, bachelors, students.

The collection included in the list of professional publications (SCA Ukraine Resolution of 10/03/2010. № 1-05/2). Founded by a decision of the Academic Council of «KPI», protocol № 4 from 03/04/2000.

Responsible for release: Prokofiev M. I., director SRC «TESIS»

Worked on the release of editor: Kulii R. O.

Editorial address and publisher:
National Technical University of Ukraine
«Igor Sikorsky Kyiv Polytechnic Institute»
Scientific Research Center «TESIS»
03056, Ukraine, Kyiv, prospekt Peremogi, 37
(vul. Politekhnichna, 12), block 17, of. 406
tel. (044) 204-86-25, tel./fax (044) 204-83-85. E-mail: pnzzi@tesis.kiev.ua

Scientometric base: *Ulrichweb Global Serials Directory, Scientific Periodicals Ukraine, OJS, Base, EZB, ELAKPI, Vernadsky National Library of Ukraine, Institute for information recording*

The collection is registered in the State Committee for Information Policy, Television and Radio Broadcasting of Ukraine. Certificate KB № 5185 from 12/06/2001.

Certificate of registration «KPI» the State Register of publishers, manufacturers and distributors of publishing products number 211 series DK.

Issued by the decision of the Academic Council of Igor Sikorsky Kyiv Polytechnic Institute.
Signed for publication 14/07/2017. The circulation of 100 copies. Format 60x84 / 8. Disc.-publ. pp. 18.7.
Order number 07-2 of 17/07/2017.

З М І С Т

4. Технічні засоби системи захисту інформації. Визначення відповідності засобів ТЗІ

5. Підготовка та підвищення кваліфікації спеціалістів систем захисту інформації

C O N T E N T

1. Problems of regulatory and metrological bases of information security

2. Cybersecurity and critical information infrastructure protection

3. Ensuring information security in information systems

4. Technical means of information protection system. Consistency means TSI

5. Preparation and advanced training specialists of information security systems

1. Проблеми розвитку нормативної та методичної баз системи захисту інформації

УДК 004.43(031):681.3.01(02)

МОЖЛИВІСТЬ АВТОМАТИЗАЦІЇ ПРОЕКТУВАННЯ КСЗІ

Луценко Володимир
КПІ ім. Ігоря Сікорського

OPPORTUNITY OF AUTOMATION OF DESIGNING OF CSPI

Lutsenko Volodymir
Igor Sikorsky Kyiv Polytechnic Institute

Анотація: **Аналізується можливість та особливості автоматизації проектування комплексних систем захисту інформації.**
Ключові слова: **Інформація, захист інформації, комплексна система захисту інформації, автоматизація проектування.**
Summary: **The opportunity and features of automation of designing of complex systems of protection of the information is analyzed.**
Keywords: **The information, protection of the information, complex system of protection of the information.**

Вступ

Методи аналізу й керування ризиками відрізняються помітним різноманіттям. До найбільш поширених відносять: метод CRAMM [1], метод Cobra [2], метод Risk Watch, Buddy System, EBIOS, MEHARI, OCTAVE, CORAS, Гриф і т.п., і при їх використанні необхідно враховувати ступінь адаптованості цих реалізацій до особливостей українських користувачів. Німецький стандарт BSIMT є найбільш змістовним довідником із забезпечення безпеки ІТ. Але проблемою є відсутність єдиного ДСТУ, котрий мав би адаптованість до місцевих умов роботи об'єктів, тобто до законодавства України, особливості відношень між організаціями-користувачами в рамках діючої інфраструктури, місцеві та регіональні особливості в створенні структури ІС, вимоги до робочої та звітної документації, традиції., тощо. Але розглядати ці продукти з аудиту безпеки в якості засобів проектування, тим більше автоматизованими, було б некоректно. При цьому і аудит безпеки досі є завданням, що знаходиться на етапі розробки. При використанні стандарту BSIMT визначають шляхом обстеження конкретного об'єкту великого розміру перелік загроз. Навіть маючи повний перелік можливих контрдій, залишається невирішеною головна задача – знайти відповідність між можливими контрдіями і конкретними загрозами. Це залишається завданням для проектанта з його суб'єктивністю (вподобаннями, кваліфікацією, досвідом і. т.д.). Тому і виникають зовсім різні проекти комплексних систем захисту інформації (КСЗІ) для фактично однакових об'єктів, особливо великих, розподілених територіально та функціонально залежних, або автономних.

Враховуючи складності, які виникають в даному випадку на шляху автоматизації проектування КСЗІ, виникає питання – а чи є така можливість за умови єдності прийняття рішень проектантом доказової однозначності (об'єктивності таких рішень), мінімізації фінансового навантаження на результат проектування, тобто, на спроектовану систему захисту за умови достатності рівня захищеності об'єкту захисту (ОЗ)?

Формалізація складових проектування як об'єктів захисту

Початковим етапом завдання автоматизації проектування КСЗІ є етап формалізації складових проектів, тобто всіх можливих об'єктів автоматизації. Визначення, які наведені у статті можуть відрізнятись від загальноприйнятих і слугують для постановки задачі автоматизації проектування систем захисту. Зокрема це стосується об'єктів інформаційної діяльності (ОІД) та ін. Видів таких об'єктів декілька. Це інформаційно телекомунікаційні системи (ІТКС), об'єкти, які не вміщують у своєму складі ІТКС, наприклад, за визначенням, виділені приміщення (ВП), які будемо називати для спрощення просто ОІД, та уся сукупність комбінацій ІТКС та ОІД, яку для спрощення будемо називати об'єктами захисту загальної структури (ОЗЗС). Поєднання ОІД та ІТКС у вигляді ОЗЗС вимагає визначення мінімуму структурних варіантів типів об'єктів захисту, тобто базису структурних елементів. До них мають відноситися ті, що наведені у табл.1.

Таблиця 1.

Структури ОЗЗС

1.	ОІД, котрий не вміщує у своєму складі ІТКС
2.	ОІД, у склад котрого входить ІТКС, або декілька ІТКС, у тому числі, мережа загального користування (наприклад мережа INTERNET, або телефонна мережа)
3.	ІТКС, у склад якої входить ОІД, або декілька ОІД призначених для обслуговування ІТКС за її функціональним призначенням, або призначених також для її обслуговування за допоміжним функціональним призначенням (офісні приміщення, склади товарів, технологічні та виробничі приміщення, тощо)
4.	ОЗЗС, котрі визначені як головна ІТКС, у склад якої входить підлегла ІТКС'. У склад ІТКС' входять також і ОІД з своїм, визначеним для цього ІТКС' призначенням, що не несе функціональні обов'язки, характерні для головної ІТКС. Назвемо такі ОЗЗС гібридними ОЗЗС першого типу
5.	ОЗЗС, котрі визначені як головний ОІД у склад якого входять також і ІТКС з своїм, визначеним для цього ОІД призначенням, та ОІД' у складі цієї ІТКС. Причому, цей підлеглий ОІД' або несе, або не несе функціональні обов'язки, характерні для головного ОІД – гібридні ОЗЗС другого типу

Відсутність ІТКС як окремої структурної одиниці зумовлена тим, що інформації без носія бути не може.

З таких структурних елементів складається структура будь-якого ОЗЗС в рамках якогось інфраструктурного рівня, наприклад окрема кімната в межах структури підприємства або установи, що дислокується у межах району, який у свою чергу є складовою структури міста, а той є складовою структури області, котра у свою чергу структурується у регіонально-територіальному масштабі чи взагалі загальнодержавному. Найпростішим варіантом структури об'єкту захисту є такий, який не пов'язаний з локальним розташуванням. Фактично, така структура і є характерною, але наразі створення служби захисту інформації (СЗІ) та КСЗІ об'єктів захисту здійснюється без урахування їх приналежності до загальної структури цих об'єктів. Тобто, наприклад, характерним є випадок, коли розробляється КСЗІ ОІД у вигляді нового регіонального офісного приміщення. Це офісне приміщення є фрагментом більш загальної структури, наприклад системи зв'язку ІТКС', яка у свою чергу входить у більш загальну ІТКС для системи мобільного зв'язку (гібридний ОЗЗС першого типу). При цьому для цієї ІТКС КСЗІ вже є розробленою та діючою системою. Але розробка КСЗІ даного нового офісу може здійснюватися незалежно від КСЗІ його ІТКС, у тому числі і різними виконавцями. При цьому формуються умови життєдіяльності ОІД, вимоги до СЗІ, модель загроз, і.т.д., хоча ця робота вже є

проведеною для усього ОЗЗС і немає ніяких гарантій того, що проект захисту даного офісу буде вміщувати складові, що не мають протиріч з КСЗІ ІТКС. Загалом, КСЗІ офісу має повторювати пункти КСЗІ його ІТКС, або має створюватися як копія фрагменту КСЗІ його ІТКС. Таким чином, КСЗІ складних об'єктів має виглядати як ієрархічна структура жорстко пов'язаних між собою КСЗІ об'єктів нижнього рівня, узагальнення пунктів КСЗІ котрих складає КСЗІ об'єктів наступного, вищого рівня, і так далі до КСЗІ загального ОЗЗС. В інших випадках, навпаки, КСЗІ загального ОЗЗС має розподілятися на свої фрагменти у вигляді КСЗІ його ОІД та КСЗІ його ІТКС і знову ж таки створювати ієрархічну структуру у котрій об'єкт захисту нижнього рівня є відповідним фрагментом КСЗІ ОЗЗС. У будь якому випадку КСЗІ нижнього рівня не може вміщувати будь-яких вимог, яких немає у КСЗІ вищого рівня.

Таким чином, щодо правил формування КСЗІ складних об'єктів, то з огляду на викладене вище можна визначитися з положеннями щодо підходу до проектування КСЗІ у випадках коли ОЗЗС є розгалуженою однорівневою і коли ОЗЗС є ієрархічною багаторівневою структурою.

Якщо застосовувати структурний підхід, то тоді правила формування КСЗІ для ОЗЗС [3] можуть формулюватися для випадків, згідно табл. 2.

Таблиця 2.

Правила формування КСЗІ

Для ієрархічного розподіленого ОЗЗС:	
a) Випадок, коли ОЗЗС будується починаючи з нульового, вищого рівня структури, передбачаючи ієрархічність структури, що створюється, або обстежується	
1	До складу ТЗ на КСЗІ вищого рівня мають входити усі загальні вимоги до ТЗ КСЗІ нижчих рівнів
2	До складу ТЗ на КСЗІ нижчих рівнів не можуть включатися будь-які вимоги, котрі є відсутніми у складі ТЗ на КСЗІ нульового рівня
3	Проект КСЗІ для вищого рівня ОЗЗС має вміщувати у своєму складі проекти КСЗІ всіх об'єктів захисту нижнього рівня у якості своїх складових
b) Випадок, коли ОЗЗС будується починаючи з нижчого рівня структури, а майбутня ієрархічність загальної структури ОЗЗС є невизначеною	
1	КСЗІ для окремих ОЗЗС визначеного рівня створюються незалежно один від одного та без урахування майбутньої ієрархічності структури ОЗЗС
2	При появі фрагменту ОЗЗС наступного, вищого рівня, ТЗ на його КСЗІ та проект захисту створюється як сукупність пунктів ТЗ та проектів КСЗІ об'єктів нижчого рівня
3	ТЗ та проекти КСЗІ об'єктів вищого рівня можуть включати пункти, специфічні для ОЗЗС даного рівня за умови, якщо вони не мають протиріч з ТЗ та КСЗІ, визначених для будь-яких ОЗЗС нижчих рівнів
4	ТЗ та проект КСЗІ для ОЗЗС кожного наступного рівня має вміщувати усі пункти ТЗ та проектів КСЗІ, які були визначеними для усіх ОЗЗС попередніх, більш нижчих рівнів, у тому числі, специфічні за п.3 даного переліку, для попереднього рівня
Для однорівневого розподіленого ОЗЗС	
1	ТЗ та проект КСЗІ розробляється для кожного ОЗЗС незалежно один від одного
2	Пункти ТЗ та проектів КСЗІ будь-якого ОЗЗС не повинні мати протиріч з будь-якими пунктами ТЗ та проектів КСЗІ інших ОЗЗС
3	ТЗ та пункти проектів КСЗІ, що є специфічними для окремого ОЗЗС структури, додаються до його ТЗ та проекту КСЗІ у вигляді окремого пункту, тобто не можуть включатися як підпункт до вже існуючого переліку пунктів, визначених для інших ОЗЗС даної структури

При виконанні таких правил виникає можливість створення КСЗІ будь-яких видів ОІД, які складатимуть єдину технологічно-інформаційну структуру будь-якого рівня, у тому числі і державного рівня. В таку структуру включаються усі ОІД незалежно від їх призначення, масштабу та складності. Крім того, вперше з'являється реальна можливість створення методології побудови КСЗІ будь-якої складності у тому числі і за рахунок використання автоматизованої системи проектування. Тобто процес проектування отримує принципову можливість автоматизації за єдиною універсальною методикою.

За такого підходу, та при умові розробки відповідних ДСТУ і нормативно - методичної документації, з'являється можливість створення єдиного методу проектування ОЗЗС, що відрізняється досконалістю за рахунок прийняття рішень при реалізації проекту, незалежних від суб'єктивних властивостей проектанта.

Нагальність створення такого методу є безумовною, оскільки у діючій методиці проектування СЗІ (КСЗІ для АС ІТКС) базою є комплект ДСТУ, нормативні та методичні документи, що у своїй сукупності характеризуються взаємною неузгодженістю [4]. Наразі проекти КСЗІ створюються в умовах об'єктивної неможливості виконання усіх вимог діючої нормативно-методичної документації, а підхід, що розглядається, передбачає можливість вирішення зазначених протиріч.

Визначення та правила щодо моделювання комплексних систем захисту інформації

Змістовно, для будь-якого ОЗЗС, структура, яка ілюструє процедуру проектування, може бути представленою як на рис. 1.

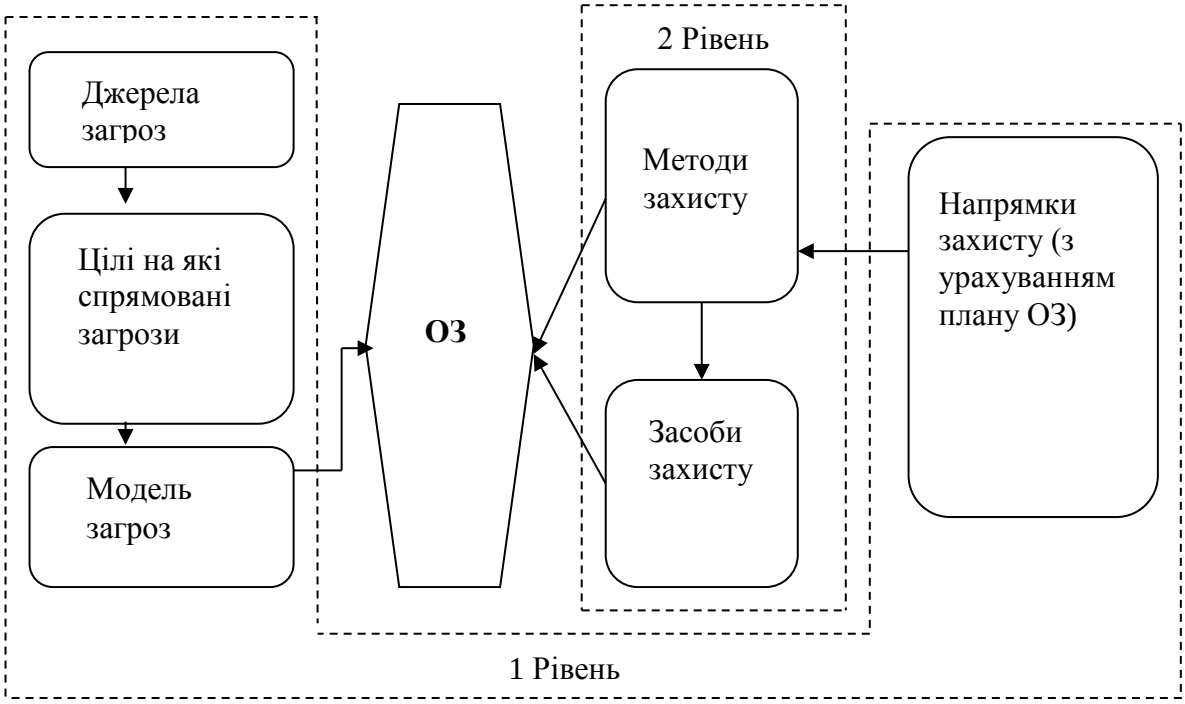


Рис. 1 – Варіант узагальненої структури проектування КСЗІ

Вхідним чинником для визначення структури КСЗІ є перелік I елементів $i \in I$, з яких складається об'єкт, що вимагає захисту, та стан S(I) множини цих елементів I, що визначаються на рівні «1» проектування згідно рис.1. Для створення переліку засобів та методів ЗІ (контрдій на рівні проектування «2» згідно рис. 1) є стан таких елементів $S(I_i)$, тобто i-й варіант переліку I, і відповідний перелік дестабілізуючих факторів (DF) для

кожного стану (тобто загроз). Саме ці два фрагменти послідовності проектування є такими, які не можуть бути жорстко алгоритмовані за рахунок введення переліку правил переходів від DF до загроз, та від загроз до засобів ЗІ, тобто вимагають використання підходів на засадах сітьового моделювання з використанням «пам'яті з адресацією за змістом запиту» . При цьому засоби захисту можуть розглядатися і як рішення про використання технічних пристроїв, і як рішення про використання такого методу захисту, для якого його технічна реалізація є однозначно регламентованою процедурою, тобто такою, що виконується згідно відомої діючої методики відомими засобами. Якщо означити перелік DF як $F=(\text{the list DF})$, тоді: $F=f(S(I))$, а перелік засобів та методів захисту для кожного окремого випадку ОЗЗС (підмножинаY_i) з загальної сукупності відомих методів та засобів (множина Y) використовує вибірку F в якості свого аргументу, тобто $Y_i = f(F_i(S(I)))$, де *i* є знаком приналежності до конкретного випадку ОІД чи ІТКС. З цього витікає, що процедура визначення переліку F_i та процедура визначення засобів та методів захисту Y_i є послідовністю двох процедур (два етапи проектування). На першому етапі визначається перелік загроз ОЗЗС, а на другому етапі здійснюється пошук технічних засобів та методів ЗІ. Різні автори по різному представляють поняття DF та поняття загроз, тобто, або ототожнюють їх, або розділяють. Якщо ототожнити DF та їх причини як загрози, тоді на їх основі можна визначати групи порушень, що можуть бути визначені з реалізацією загроз. Якщо розділити DF та їх причини, то тоді вводять поняття DF та джерел DF. При цьому частіше за все для ІТКС до причин DF відносять людський фактор (окремі особи, або групи осіб, які мають відношення до порушень захищеності інформації), технічні пристрої, математичне забезпечення (моделі, алгоритми, програми), технологію функціонування АС (рішення конкретних задач), зовнішнє середовище. До DF відносять можливий результат дії причин у вигляді кількісної недостатності, якісної недостатності, відмов, збоїв, помилок, стихійного лиха, зловмисних дій та побічних явищ. Але для ОЗЗС у вигляді ОІД такі визначення не є логічними. Тому єдність у підході до проектування вимагає визначення DF фактично як джерела DF, а загрозами будемо визнавати і DF і відповідне формулювання описів загроз, що не входять до DF. Тоді термінологія та змістовний сенс загроз та DF стає єдиним для будь-якої структур ОЗЗС, таких які наведені у табл. 1. Крім того, за такого підходу при створенні моделі проекту КСЗІ забезпечується єдність у описі DF та загроз і для структури системи захисту ОЗЗС технічними каналами і для структури системи захисту ОЗЗС від несанкціонованого доступу (НСД).

Таким чином, формується множина опису елементів ОІД ($i \in I$), їх стану S(*I*), переліку DF ($F=f(S(I))$) та рішень щодо засобів та методів захисту $Y_i = f(F_i(S(I)))$. Множину опису елементів ОІД можна характеризувати як декотрий образ об'єкта. Сукупність опису мають складати відповідні бази даних (БД).

Базис структур ОЗЗС та визначення засобів захисту

Кожний елемент ОІД представляється у вигляді відповідного образу (наприклад, переліку, або діаграми) його властивостей *i* з загальної множини образів елементів об'єкту I, $i \in I$. Змістовно кожна властивість *i* є визначенням (деяким текстом, фразою або декількома фразами), що описується розробником (випадок втручання оператора) як деякий елемент об'єкту. Кожна окрема фраза *i* має сенс одної з властивостей елементу об'єкту. Так, окремий комп'ютер має опис, що може складатися з таких фраз:

*i*1 – обчислювальна машина персональна; *i*2 – типом машини є машина загального користування (або серійна, або неспеціалізована, тощо); *i*3 – фірмою виготовлювачем є фірма IBM (або Siemens Nixdorf, або інша); *i*4 – призначенням є виготовлення документів з грифом ДСК (або таємно, або цілком таємно, тощо); *i*5 – місце розташування і.т.д.

Тоді набір таких *i*-фраз (або окремих слів) і є образом елемента (специфікація властивостей елемента) даного об'єкта. Фрази можуть формуватися довільно, або з деякої кінцевої бібліотеки (множини) фраз, тобто з бази даних БД описів елементів. У будь-якому випадку будемо вважати, що БД вміщує загалом I можливих фраз $i \in I$ (їх іноді називають реалізаціями фраз). Тоді відповідна сукупність таких реалізацій визначає стан відповідного елемента об'єкта $S(I_i)$ з усієї сукупності можливих станів $S(I)$ усіх можливих елементів (тобто: $S(I_i) \in S(I)$, що і є визначеним вище. Формально, така реалізація $S(I_i)$ також є образом стану.

На таких засадах види об'єктів захисту та базис структур ОЗЗС (за табл.1) можна представити у вигляді діаграм Ейлера-Вена (рис. 2 та 3 відповідно).

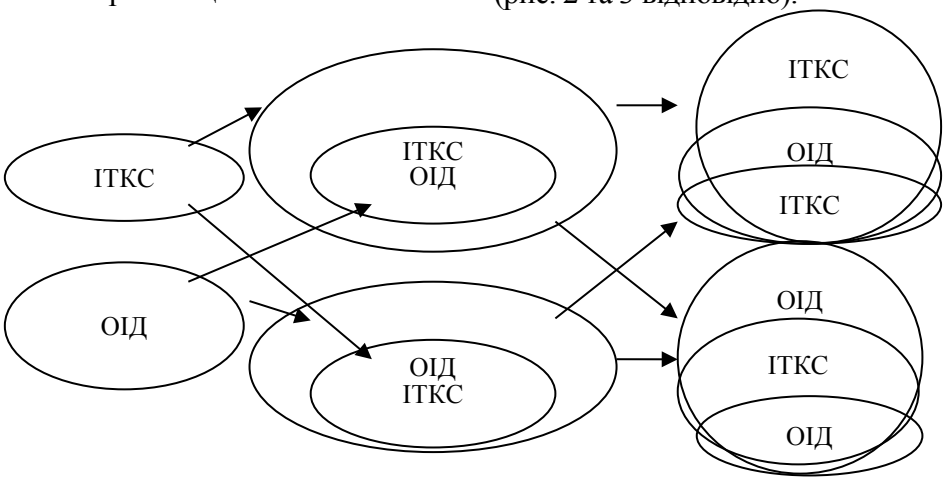


Рис. 2 – Види об'єктів захисту

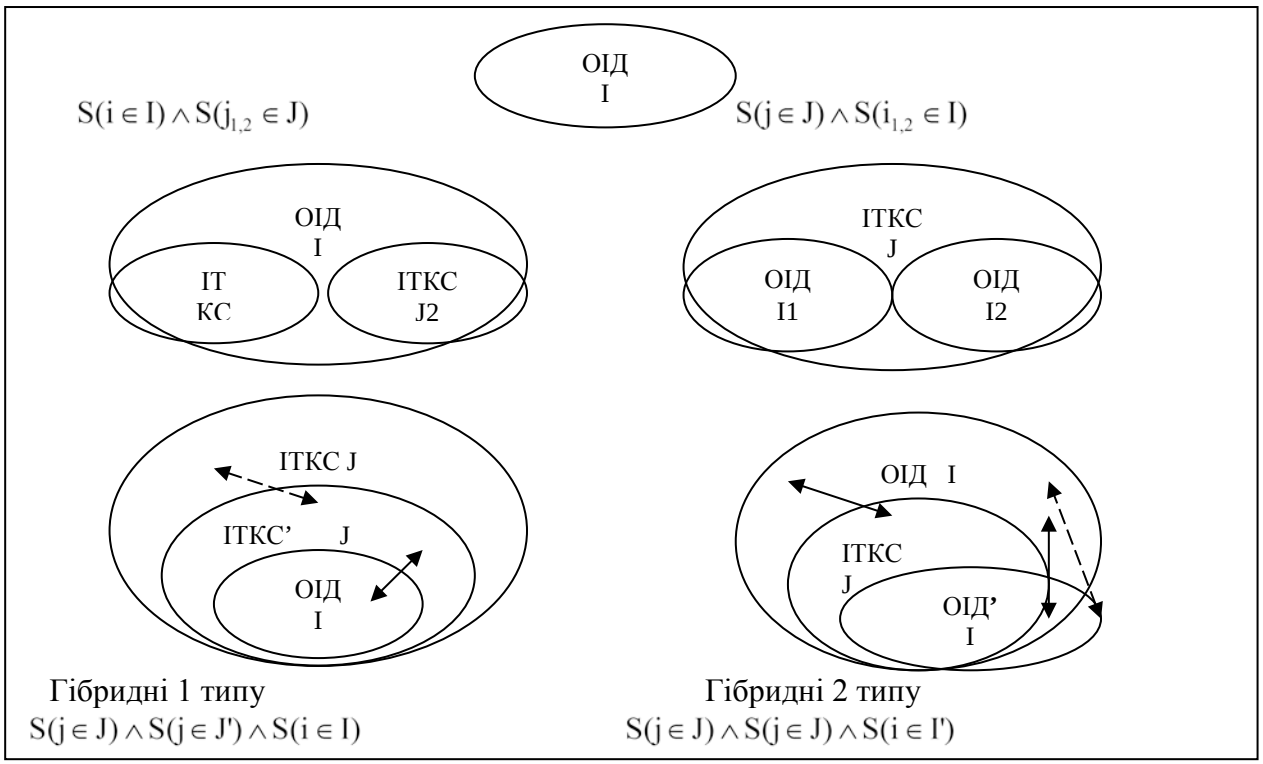


Рис. 3 – Базис структур ОЗЗС
$I_1, I_2, \ldots, I_N$ – образи елементів об'єктів захисту №№ 1, 2,…,N типу ОІД;
$J_1, J_2, \ldots, J_N$ - образи елементів об'єктів захисту №№ 1, 2,…,N типу ІТКС.

Якщо БД DF створювати аналогічним чином, то тоді перелік *F* (тобто – специфікація або образ як сенсовий зміст специфікації) тих DF, які відносяться до даного елемента даного об'єкту і отримані в результаті «спеціального обстеження» дослідником – розробником (випадок втручання оператора) загалом є вибіркою, що залежить (є деякою функцією) від стану S елемента *I* , тобто $F=f(S(I))$.

Сенсовий зміст F є функцією зв'язку між станом елементу об'єкту та отриманою специфікацією DF_i з сукупності можливих специфікацій DF $(DF_i \in DF)$. Специфікацію DF (образ DF_i для даного *i*-го елемента) логічно позначати F_i. Тоді, за визначенням формальних зв'язків, загрозою Y для даного *i*-го елемента є образ Y_i, котрий визначається як вплив $DF_i \in DF$ на стан S(*I*). Логічний зв'язок між образом загрози та образом стану з відповідними DF може бути представлений як: $Y_i=f(DF_i \wedge S(i \in I))$, де: - символ $\wedge$ є кон'юнктивною функцією (поєднання множин); функція f є функцією зв'язку між сенсовим змістом стану елемента та впливом DF на нього.

Можливим є представлення множин елементів що відтворюють зазначені образи, у вигляді діаграм Ейлера-Вена (рис. 4 та 5).

Рис. 4 – Представлення окремих образів *I,* DF та S

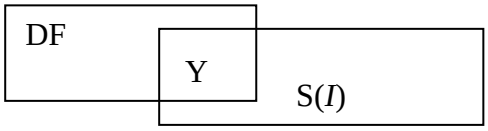


Рис. 5 – Представлення образу загроз Y

Специфікація загроз, які створюють образ загроз, є вихідними даними для подальшого визначення засобів ЗІ, що складають результуючу мету проектування.

Образ загроз Y визначає напрямки захисту, але для визначення засобів захисту необхідно спиратися на можливості протидії загрозам, а саме на БД можливих засобів захисту, що складають образ БД. Позначимо БД можливих засобів захисту образом Z. Таким чином, виділення з БД засобів захисту (множини засобів) тієї частини засобів, котра є необхідною для обслуговування поточного ОЗЗС, становить завдання визначення відповідної підмножини $Z_i \in Z$. Підмножина Z_i є образом засобів захисту поточного ОЗЗС. Відповідним образом загроз поточного ОЗЗС є підмножина $Y_i \in Y$.

Множина засобів захисту як образ Z складається з чотирьох кластерів (образів підмножин) засобів, до яких можуть відноситися активні засоби захисту $Z(A_i)$, пасивні засоби захисту $Z(P_i)$, заборони (обмеження) у використанні тих чи інших засобів (у найбільшій мірі – активних) $Z(N_i)$, криптографічні засоби $Z(K_i)$, яке представлено на рис. 6.

Тобто образ усіх можливих засобів Z складається з чотирьох образів Z(A,P,N,K). Початковими умовами використання засобів захисту при проектуванні Z(A,P,N,K є образ усіх можливих засобів, а кінцевим результатом проектування є відповідний до поточного ОЗЗС образ засобів $Z(A_i,P_i,N_i,K_i)$. Символ *i* означає відповідність образів засобів захисту до образу загроз $Z_4(A_i) \in Z(A)$ $Y_i \in Y$ поточного ОЗЗС.

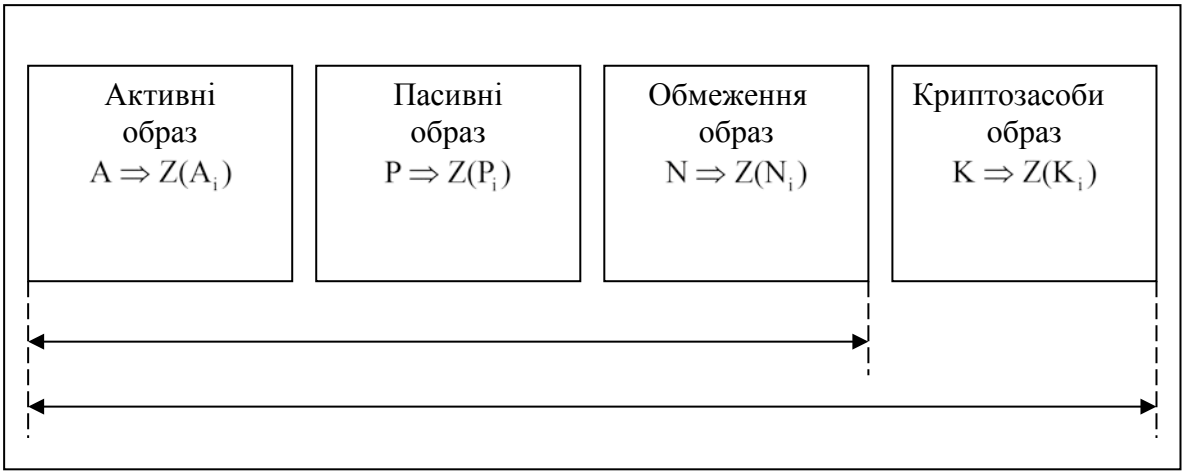


Рис. 6 – Кластери засобів захисту ОЗЗС

Розглядаючи процедуру визначення засобів захисту як пошукову процедуру в термінології кінцевих автоматів FSM (FSM – Finite State Machines), визначимо початковий стан образом $Y_i \in Y$, кінцевий стан – образом $Z(A_i,P_i,N_i,K_i)$, а інструментом переходу з початкового до кінцевого стану є алгоритм роботи АП як предикат АП. Необхідно визначити умови, за якими можливою є процедура переходу від початкового до кінцевого стану, тобто існування квантора:

$$\forall(Y_i \in Y)\ \exists\ (Z(A_i,P_i,N_i,K_i))=\text{TRUE}$$

Для цього розглянемо варіанти можливих образів підмножин засобів захисту для ОЗЗС довільної архітектури.

$$(Y_i \in Y) \rightarrow Z(A,P,N,K) = \begin{cases} Z(P) \leftrightarrow \neg Z(A) \wedge \neg Z(K) & (1) \\ Z_1(A_j) \in Z(A) \leftrightarrow \neg Z(N) \wedge \neg Z(K) \wedge \left[Z(P) \vee \left(Z(P_j) \notin Z(P) \right) \right] & (2) \\ Z_2(A_i) \in Z(A) \leftrightarrow \neg Z(N) \wedge \neg Z(K) \wedge Z(P) & (3) \\ Z_3(A_i) \in Z(A) \leftrightarrow \neg Z(N) \wedge Z(P) \wedge Z(K) & (4) \\ Z_4(A_i) \in Z(K) \leftrightarrow \neg Z(N) \wedge \neg Z(P) & (5) \\ Z(P) \leftrightarrow \neg Z(A) \wedge Z(K) & (6) \\ Z(K) \leftrightarrow \neg Z(A) \wedge \neg Z(P) & (7) \end{cases}$$

Тут символ j підкреслює приналежність тільки до тієї частини j-х активних засобів, які дозволяють компенсувати недостатність пасивних засобів $Z(P_j) \notin Z(P)$. Цим виразом виділення образу Z(A,P,N,K) як події, котра відбулася в результаті події, що створила стан ($Y_i \in Y$), підкреслюється, що образи загроз є аргументом майбутньої появи образу засобів захисту Z(A,P,N,K).

Наведені вирази (1) – (7) мають відповідні відображення у вигляді діаграм Ейлера-Вена, наведені для поточного ОЗЗС за рис.7.

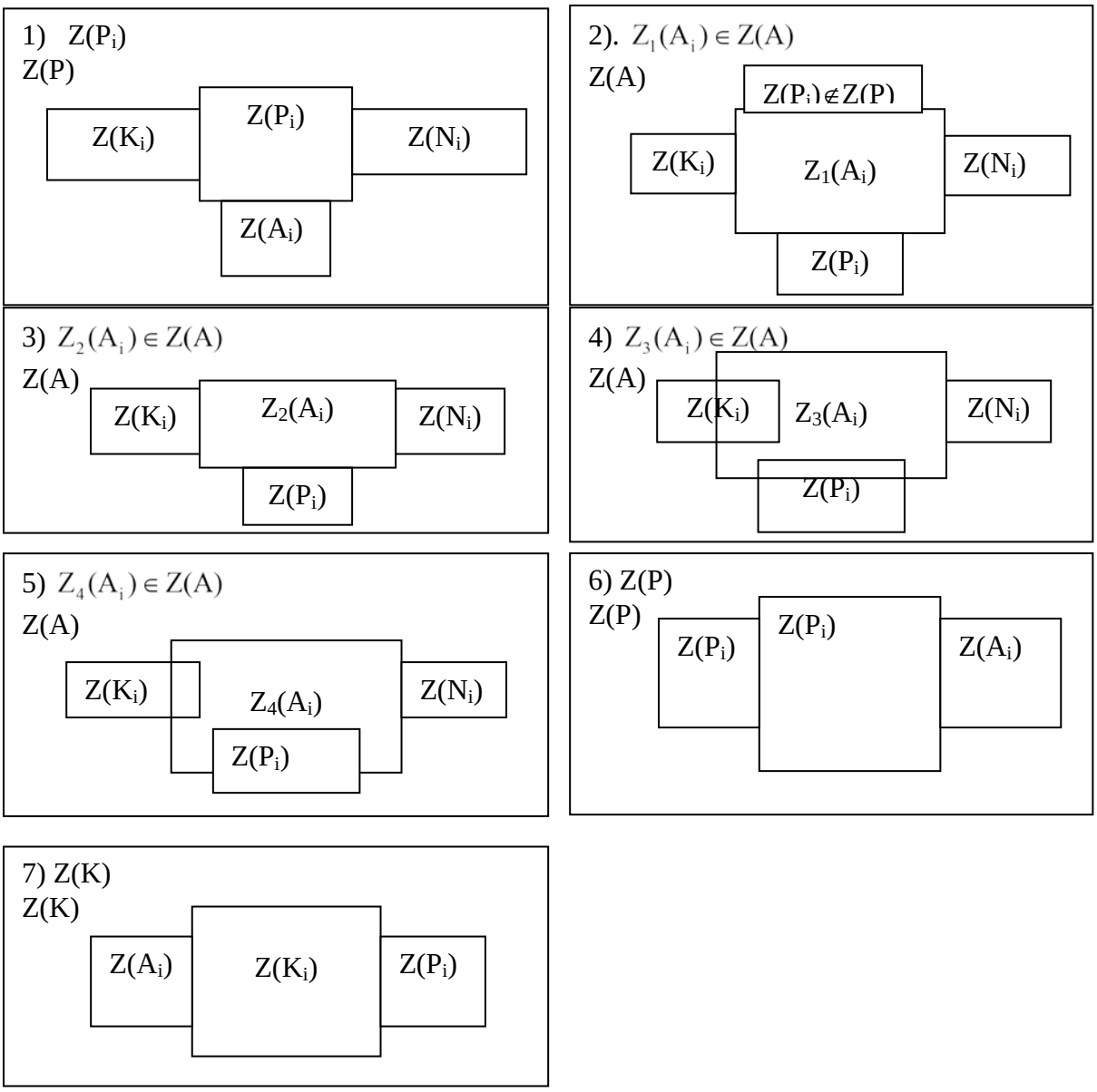


Рис. 7 – Діаграми Ейлера-Вена за виразами (1) – (7)

Вирази (1) – (7) мають сукупний сенс при умові введення деяких заборон та обмежень, наведених в табл. 3. Тобто при умові, коли заборони та обмеження N є апріорно визначеними для будь-якого об'єкту у вигляді кінцевої специфікації і з аргументу Z переводиться до параметру {Z(A,P,K),N=const}.

Таблиця 3.

Заборони та обмеження щодо використання активних засобів

1. Активні засоби Z(A) використовуються тільки при доведеній неможливості використання пасивних засобів Z(P), або коли вже залучені пасивні засоби Z(P) об'єктивно не здатні забезпечити необхідний заданий результат захисту, що може ілюструватися загальним виразом $Y_i \in Y$. За такої умови *i* наведений вираз $Z(P_j) \notin Z(P)$, а символ *j* підкреслює, що вибірка Y_i з символом *i* не має відношення до формування такої забороненої вибірки $Z(P_j)$. Тоді стає зрозумілим, що номери 1,2,3 та 4 у визначенні $Z_1(A_j)$, $Z_2(A_j)$, $Z_3(A_j)$ та $Z_4(A_j)$ відповідно, означають випадки:
а) Z_1 – випадок, коли активні засоби використовуються без пасивних засобів (або визначені

пасивні не забезпечили необхідний результат) та без криптометодів. б) Z_2 – випадок, коли активні засоби застосовуються разом з пасивними засобами при відсутності криптометодів та відсутності заборон на активні засоби. в) Z_3 – випадок використання активних разом з пасивними засобами та криптографічними. г) Z_4 – випадок, коли активні засоби суміщені виключно з криптографічними.
2. Заборони та обмеження Z(N) поширюються тільки на активні методи захисту. Загалом, активні методи захисту мають наступні недоліки: а) використання активних методів захисту приводить до нездоланних демаскуючих признаків об'єкту. б) наявність засобів активного захисту порушують електромагнітну сумісність наявних на об'єкті технічних засобів. в) за умов використання багатоканальних засобів перехоплення та довготривалому накопиченні інформації що перехоплюється засобами розвідки зберігається можливість виділення інформативних компонентів з сигналів що захищаються і вірогідність позитивних або негативних наслідків атаки не є визначеною. г) за умови використання активного захисту для захисту оточуючого простору радіоканалом медичні показники присутності є негативними. д) у присутності криптозахисту зашумлення радіоефіру не має сенсу.
3. Забезпечення необхідної та достатньої величини ентропійного коефіцієнту якості шуму, який утворюють активні засоби захисту, вимагає достовірної доведеності.

Зазначені недоліки та обмеження активного захисту, наведені в пункті 2 табл. 3, повністю підтверджують змістовність обмежень, наведених у пункті 1 табл. 3.

До пасивних засобів захисту тут відносяться засоби захисту від витоку каналами ПЕМВН та акустичними каналами, а також заходи та засоби захисту від НСД до носіїв інформації. Поєднання Z(P) з захистом від НСД не створює протиріч з загальною методологією ТЗІ.

Якщо розглянути п'ять типів структур ОІД, наведених у Таблиці 1, то тоді застосування виразів (1) – (7) до кожної з них дозволяє систематизувати образи засобів захисту для різних структур ОЗ:

1. Для структури 1 згідно таблиці 1 з загалу виразів (1) – (7) виділяються пасивні засоби та пасивні засоби у присутності дозволених активних засобів типу Z_2.

$$Z(A_i,P_i,N_i,K_i)=\begin{cases} Z(P) \leftrightarrow \neg Z(A) \wedge \neg Z(K), \\ Z_2(A_j) \in Z(A) \leftrightarrow \neg Z(N) \wedge \neg Z(K) \wedge Z(P). \end{cases}$$

Можливим є поєднання цих двох виразів за формулою логічних зв'язків:

$$Z(A,P,N,K)=Z(P) \vee \{Z(P) \wedge [Z_2(A_i) \wedge \neg Z(N)]\}.$$

2. Для структури 2 згідно табл. 1 можливим є використання дозволених активних типу Z_2 засобів у присутності пасивних або пасивні засоби та засоби криптографічного захисту.

$$Z(A,P,N,K) = Z(P)\ [\ Z2(Ai)\quad Z(K)],$$

або:

$$Z(A,P,N,K) = Z(P) \wedge [Z_2(A_i) \vee Z(K)].$$

3. Для структури 3 згідно табл. 1 можливим є використання пасивних методів захисту, поєднаних з криптографічними та дозволених активних типу Z_2 у присутності пасивних методів:

$$Z(A_i,P_i,N_i,K_i) = \begin{cases} Z(P) \leftrightarrow \neg Z(A) \wedge Z(K), \\ Z_2(A_j) \in Z(A) \leftrightarrow \neg Z(N) \wedge \neg\ Z(K) \wedge Z(P). \end{cases}$$

4. Для структури 4 згідно табл. 1 можливим є використання пасивних методів захисту, поєднаних з криптографічними, та дозволених активних типу Z_2 у присутності пасивних

методів. А це співпадає з використанням методів захисту для 3 структури.

5. Для структури 5 згідно таблиці 1 можливими є два варіанти. Якщо ОІД' не має загального призначення з головним ОІД, тоді він не має загального призначення і з ІТКС. Тобто ОІД є окремим об'єктом захисту і для нього можливим є використання методів захисту зазначених для 1 структури. Якщо ж ОІД', входячи до складу ІТКС, має загальне призначення з головним ОІД, то тоді призначення ОІД' співпадає з призначенням ІТКС і для нього можливим є використання методів захисту, зазначених для 3 структури.

Оскільки $Z(A_i,P_i,N_i,K_i)$ для структури 3 як виявляється є комбінацією засобів, що використовуються в якості засобів захисту для структур 1 та 2, то загальний вираз логічних зв'язків для сукупності розглянутих структур має вигляд:

$$Z(A,P,N,K) = Z(P) \wedge [Z(K) \vee Z_2(A_i)] \leftrightarrow \min[Z(P), Z(K) \vee Z_2(A_i)] . \quad (8)$$

Можливість зведення (1) – (7) до лаконічного виду (8) має логічне обґрунтування. Дійсно, оскільки активні методи мають обмеження за пунктом 1 таблиці 3, то тоді засоби, зазначені формулами (2), (4) та (5), можуть не використовуватися. Відсутність (7) логічно пояснюється тим, що виключно криптографічний метод захисту ОІД в рамках розробки КСЗІ не має сенсу з причини відсутності логіки для випадку, коли інформаційний потік захищається, а носій інформації відсутній. Теоретично існують два випадки, коли можливим є використання виключно криптографічного методу захисту. Ще один випадок, це використання окремого пристрою (чи абонентського комплекту) захисту *мовної* інформації, такого, як маскіратор, скремблер, вокодер або ліпредер у телефонних каналах зв'язку, або при використанні приймально-передавальної апаратури (рації) у радіоканалі сумісно з зазначеними пристроями. Іншим випадком є використання пристроїв спеціального зв'язку при виконанні тактичних операцій підрозділами спеціального призначення. В обох випадках ніякої мови про КСЗІ не йдеться по причині фактичної відсутності об'єкту захисту, або ІТКС.

Висновки

Права частина виразу (8) $\min[Z(P),Z(K) \vee Z_2(A_i)]$ змістовно означає, що при виконанні 4-х умов, а саме:

1. коли об'єкти захисту представити згідно структурам ОЗЗС;

2. структури ОЗЗС класифікувати за типами згідно табл. 1;

3. при умові використання засобів захисту на засадах обмежень та заборон згідно табл. 3;

4. на трьох наступних етапах проектування:

- *визначення загроз та контрдій;*
- *визначення зв'язку між складовими переліку порушень та кожною складовою КСЗІ;*
- *при процедурі визначення технічних засобів захисту за напрямками захисту.*

Необхідно використовувати саме пам'ять з адресацією за змістом запиту у якості БД DF, БД порушень та БД методів та засобів захисту. Тоді за результатом проектування має бути прийнятим рішення щодо використання методів та засобів захисту у їх мінімальному об'ємі. Це автоматично мінімізує і фінансове навантаження на систему захисту в цілому.

Наявність єдиного рішення за виразом (8) свідчить також про те, що при проектуванні за зазначеною логікою доцільно вважати доведеним унеможливлення ситуації, коли однакові, або майже однакові об'єкти, отримують зовсім різні рішення щодо їх КСЗІ.

Таким чином предикат (8) є достатнім єдиним виразом, котрий описує логіку вибору при комплектуванні системи захисту будь-якого ОЗЗС. Враховуючи вираз (8) можна вважати, що алгоритм формування БД DF, БД загроз, БД засобів захисту та зв'язків між ними з логікою роботи є таким, який повинен та може привести до прийняття єдиного для кожного окремого ОЗЗС рішення. Причому сам вираз (8) не є описом послідовності дій, за якою визначається процес моделювання.

Доведеність дійсності предикату (8) означає, що для будь якого реального об'єкту (тобто такого, для якого виконуються обмеження згідно табл. 3) існує тільки одне рішення у виборі методів та засобів захисту, котре об'єктивно має логічний сенс, має властивість достатності обраних методів та засобів захисту для вирішення задачі захисту та не включає у свій склад зайвих, повторюваних елементів захисту. Тобто для таких об'єктів існує рішення з ознаками об'єктивності. У це і вкладається сенс достовірності та оптимальності рішень при проектуванні.

Перелік посилань

[1] BS 7799:1995 – *Code of practice for information Security Management BS 7799.* http://bezpeka.ladimir.kiev.ua/pg/show/risks/page2.html.

[2] ГОСТ Р ИСО/МЭК 17799-2005 *«Информационная технология. Практические правила управления информационной безопасностью»*.

[3] В. М. Луценко, *Комплексні системи захисту інформації довільної складності* / Луценко Володимир Миколайович // «Захист інформації». наук. тех. журнал. К.: – 2012. - НАУ, №2 (55). - с. 15-18.

[4] В. М. Луценко, *Відповідність етапів побудови систем захисту інформації стадіям створення автоматизованих систем* / Луценко Володимир Миколайович // «Захист інформації». Наук. тех. журнал. – К.: - 2011. НАУ, №3 (52). - с.52-56.

References

[1] BS 7799:1995 – *Code of practice for information Security Management BS 7799.* http://bezpeka.ladimir.kiev.ua/pg/show/risks/page2.html.

[2] HOST R YSO/МЭК 17799-2005 *«Ynformatsyonnaia tekhnolohyia. Praktycheskye pravyla upravlenyia ynformatsyonnoi bezopasnostiu»*.

[3] V. M. Lutsenko, *Kompleksni systemy zakhystu informatsii dovilnoi skladnosti* / Lutsenko Volodymyr Mykolaiovych // «Zakhyst informatsii». nauk. tekh. zhurnal. K.: – 2012. - NAU, №2 (55). - s. 15-18.

[4] V. M. Lutsenko, *Vidpovidnist etapiv pobudovy system zakhystu informatsii stadiiam stvorennia avtomatyzovanykh system* / Lutsenko Volodymyr Mykolaiovych // «Zakhyst informatsii». Nauk. tekh. zhurnal. – K.: - 2011. NAU, №3 (52). - s.52-56.

Реферат

Луценко Володимир

Можливість автоматизації проектування КСЗІ

Аналізується можливість та особливості автоматизації проектування комплексних систем захисту інформації. Враховуючи складності, які виникають при автоматизації такого проектування, виникає питання про можливість автоматичного проектування, за умов єдності прийняття рішень проектантом, доказової однозначності (об'єктивності таких рішень), мінімізації фінансового навантаження на результат проектування, тобто, на спроектовану систему захисту за умови достатності рівня захищеності об'єкту захисту. Для вирішення такого питання наведений підхід, що дозволяє формалізувати опис будь-якого об'єкту захисту мовою теорії нечітких множин. Наведений формальний опис об'єктів захисту довільної складності. Для цього вперше введеним э поняття об'єкту захисту загальної структури. Опис можливих структур системи захисту довільних об'єктів здійснено мовою предикатів. За цей рахунок доведено, що при проектуванні систем захисту інформації за визначеною методикою для будь-якого реального об'єкту існує тільки одне рішення у виборі методів та засобів захисту, котре об'єктивно має логічний сенс, має властивість достатності обраних методів та засобів захисту для вирішення задачі захисту та не включає у свій склад зайвих, повторюваних елементів захисту. Тобто для таких об'єктів існує рішення з ознаками об'єктивності при умові мінімізації фінансового навантаження на результат проектування.

Луценко Владимир

Возможность автоматизации проектирования КСЗИ

Анализируется возможность и особенности автоматизации проектирования комплексных систем защиты информации. Учитывая сложности, которые возникают при автоматизации такого проектирования, возникает вопрос о возможности автоматического проектирования при условии единства принятия решений проектантов, доказательной однозначности (объективности принятия решений), минимизации финансовой нагрузки на результата проектирования, т.е. на спроектированную систему защиты при условии уровня защищенности объекта защиты. Для решения такой задачи приведен подход, позволяющий формализовать описание произвольного объекта защиты языком нечетких множеств. Приведено формальное описание объектов защиты любой сложности. Для этого впервые введено понятье объекта защиты общей структуры. Описание возможных структур системы защиты произвольных объектов приведено языком предикатов. За счет этого доказано, что при проектировании систем защиты информации по определенной методике для любого реального объекта существует только одно решение при выборе методов и средств защиты, которое имеет объективный логический смысл, обладает свойством достоверности в выборе методов и средств защиты и обеспечивает достаточность средств защиты в своем составе. Это означает, что для таких объектов существует решение с признаками объективности при условии минимизации финансовой нагрузки на результат проектирования.

Lutsenko Volodymir

Opportunity of automation of designing of CSPI

The opportunity and features of automation of designing of complex systems of protection of the information is analyzed. Taking into account complexities which arise at automation of such designing, there is a question on an opportunity of automatic designing under condition of unity of acceptance of decisions designers, demonstrative unambiguity (objectivity of acceptance of decisions), minimization of financial loading on result of designing, i.e. on the designed system of protection under condition of a level of security of object of protection. For the decision of such task the approach is given, allowing to formalize the description of any object of protection by language of indistinct sets. The formal description of objects of protection of any complexity is given. For this purpose the concept of object of protection of the general structure for the first time is entered. The description of possible structures of system of protection of any objects is given by language of predicates. Due to it is proved, that at designing systems of protection of the information by the certain technique for any real object there is only one decision at a choice of methods and means of protection which has objective logic sense, has property of reliability in a choice of methods and means of protection and provides sufficiency of means of protection in the structure. It means, that for such objects there is a decision with attributes of objectivity under condition of minimization of financial loading on result of designing.

Відомості про автора

Луценко Володимир Миколайович

Освіта: Вища, інженер Радіотехнік (1980).

Науковий ступінь: Кандидат технічних наук (1989).

Вчене звання: Доцент, старший науковий співробітник Національної академії наук України.

Місце роботи: Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського».

Область знань: Інформаційна безпека, кібернетика та інформаційні технології, фізика.

Наукові інтереси: Інформаційна безпека, штучний Інтелект, квантові комунікації.

Email: *lutsenkovn@ukr.net*

2. Кібербезпека і захист критичної інформаційної інфраструктури

УДК 004.491.4

БОТНЕТИ: МЕТОДИ ВИЯВЛЕННЯ ТА ПРОТИДІЇ

Сігайов Андрій; Воловик Андрій
КПІ ім. Ігоря Сікорського

BOTNETS: DETECTION AND COUNTERACTION METHODS

Sigayov Andriy; Volovyk Andriy
Igor Sikorsky Kyiv Polytechnic Institute

Анотація: **Розглянуті історія ботнетів, їхня типова архітектура, тенденції розвитку. Надані рекомендації щодо їхнього виявлення та знешкодження.**
Ключові слова: **Ботнети, виявлення ботнетів, протидія ботнетам, інформаційна безпека, безпека комп'ютерних мереж.**
Summary: **Botnets' history, their typical architecture and evolution trends are surveyed. Recommendations for their detection and counteraction are proposed.**
Keywords: **Botnets, botnet detection, botnet counteraction, information security, computer network security.**

Вступ

Через свої практично необмежені розміри та можливості ботнети складають одну з найбільш серйозних загроз інформаційній безпеці. Вони складаються з комп'ютерів, скомпрометованих шкідливим програмним забезпеченням, які розподілені у мережі Інтернет та використовуються зазвичай для досягнення якоїсь злочинної мети. Скомпрометовані комп'ютери утворюють кінцеві точки ботнету або "боти", які пов'язані з сервером управління (command and control, C&C) таким чином, що весь ботнет утворює єдиний інструмент для розсилки спаму, крадіжки конфіденційної інформації, DDoS-атак та інших видів кримінальної активності. Експерти вважають, що від 15 до 25 відсотків комп'ютерів, з'єднаних з Internet, об'єднані у ботнети [1].

Важливо розуміти, що боти не є уразливостями операційної системи чи прикладних програм. Вони є програмами, що поширюються подібно до хробаків або встановлюються через бекдори на скомпрометованих комп'ютерах. Що відрізняє боти від інших типів зловмисного програмного забезпечення, так це наявність каналу дистанційного управління.

Найбільш небезпечними властивостями ботнетів є здатність діяти приховано протягом тривалого часу, їхні розміри та важкість їхнього виявлення. Наприклад ботнет Gameover ZeuS заподіяв істотних збитків та руйнувань IT-інфраструктури, поки його вдалося приборкати об'єднаними зусиллями державних структур та приватних організацій. За оцінками експертів за допомогою Gameover ZeuS було вкрадено біля 70 мільйонів доларів США поки ФБР вдалося заарештувати більше 100 осіб, асоційованих з цим ботнетом. У червні 2014 року міністерство юстиції США оголосило, що в результаті міжнародного міжвідомчого співробітництва під кодовою назвою *Operation Tovar* вдалося тимчасово розірвати зв'язок між зараженими комп'ютерами та серверами керування Gameover ZeuS [2]. Сьогодні, за дев'ять років після першого спостереження, Gameover ZeuS почувається добре та існує

набагато довше ніж більшість шкідливого програмного забезпечення. З плином часу кількість ботнетів істотно зростає, а також і їхня фінансова вартість. Вони стають складнішими у своїх цілях, шляхах інфільтрації та запобігання виявленню, а також у методах атак. Ось чому зараз більш ніж коли-небудь фахівцям з комп'ютерної безпеки важливо бути добре обізнаними з методами виявлення та знешкодження ботнетів.

Історія розвитку ботнетів

Витоки ботнетів знаходяться у Internet Relay Chat (IRC) – текстовій системі організованій за каналами чатів, в який концепція бота не обов'язково передбачає шкідливу поведінку. Головною метою ботнетів був контроль спілкування у IRC-чатах. Боти були здатні інтерпретувати нескладні команди, надавати підтримку у адмініструванні, пропонувати користувачам прості ігри та інші сервіси, отримувати інформацію стосовно операційних систем, логінів, адрес електронної пошти, аліасів та ін. Вихідний код першого відомого IRC-бота під назвою Eggdrop був опублікований у 1993 р. [3] і досі продовжує розвиватися. На його основі майже одразу почали розроблятися зловмисні боти, головними цілями яких були атаки інших користувачів та серверів IRC. Трохи пізніше за допомогою таких ботів були запроваджені атаки відмови у доступі (Denial of Service, DoS) та розподіленої відмови у доступі (Distributed Denial of Service, DDoS).

Відбувалася еволюція ботів, які використовували все складніші механізми комунікації з ботмастером, новітні протоколи та більш потужні методи атак, що робило ботнети в цілому більш стійкими. Вони вже могли залишатися прихованими як черв'яки, самостійно поширюватися як віруси, запускати координовані атаки. Прикладами таких ботів є SDBot [4] та AgoBot [5]. Розробка AgoBot та його варіантів вважається тією точкою, після якої ботнети почали становити головну загрозу функціонування інтернету [6].

Сучасне покоління ботів може поширюватися через файлообмінінні мережі, однорангові мережі (peer-to-peer, P2P), додатки електронної пошти, інфіковані веб-сайти або заздалегідь встановлені бекдори. Комунікація між ботами відбувається зазвичай за різними протоколами (IRC, HTTP, P2P). Так в 2009 році ботнет Zeus заразив біля 3,6 мільйонів комп'ютерів [7]. Інфраструктура Zeus описується як "складна, розподілена та різноманітна, з окремими серверами для різних задач". У фахівців викликає тривогу той факт, що Zeus продовжує активно розвиватися. На сьогодгі описано вже більше чотирьох десятків його варіантів. Zeus активно застосовує техніки протидії виявленню: евристичні перевірки наявності антивірусів, відладчиків та віртуалізації середовища. Якщо виявляється спроба аналізу, Zeus доставляє фальшиве завантаження та інжектує рекламу, яку легко видалити. Фальшиве завантаження маскує доставку набагато серйознішого шкідливого коду.

Останнім досягнення дизайну ботнетів є Mirai, вперше виявлений у серпні 2016 року, який перетворює комп'ютери під управлінням Linux на боти з дистанційним управлінням [8]. Головною ціллю Mirai є зараження побутових пристроїв з істотною обчислюваною спроможністю на кшталт камер спостереження, TV-тюнерів, мережевих принтерів, домашніх маршрутизаторів з поганою безпекою, наприклад дефолтними паролями адміністративних облікових записів. Вихідний код Mirai було викладено у вільний доступ [9]. Після цього було зафіксовано декілька найбільших за всю історію атак DDoS, в тому числі атака 21 жовтня 2016 року на DNS-провайдера DYN. Потужність атаки сягала 1,2 Tbps та в офлайн перейшли Twitter, Spotify, Amazon, Reddit, Netflix, Airbnb, Github та інші [10]. Заражені Mirai пристрої постійно сканують інтернет у пошуках IP-адресів приладів Internet of Things (IoT). У Mirai вбудована

таблиця IP-діапазонів, які він не інфікує, включаючи приватні мережі та адреси, надані US Postal Service та Department of Defence. Коли Mirai ідентифікує уразливі пристрої, він намагається інфікувати їх за допомогою таблиці з 60 найбільш вживаних юзернеймів та паролів, встановлених виробниками за умовчанням. Інфіковані прилади продовжують нормально функціонувати, за виключенням хіба що тимчасової повільності та збільшеного споживання смуги пропускання. Пристрій лишається інфікованим до перезавантаження. Після перезавантаження, якщо пароль не змінено, пристрій буде інфіковано знову протягом декількох хвилин. В світі налічуються сотні тисяч приладів IoT з дефолтними налаштуваннями, що робить їх вразливими до інфікування.

Типові характеристики ботів

Ботмастер зазвичай зацікавлений у комп'ютерах-жертвах, які мають певні бажані характеристики, а саме: швидкісне підключення до інтернету, легка доступність, низький рівень захисту і моніторингу, віддалене розташування.

Враховуючи, що одним з головних видів активності ботнету є DDoS-атаки, боти повинні встановлюватися на комп'ютерах зі швидкісним доступом до інтернету. Смуги пропускання має вистачати для того, щоб паралізувати роботу будь-якого сервісу, підключеного до інтернет. Крім того, використання зараженого комп'ютера зі швидкісним доступом дозволяє практично будь-якій шкідливій активності лишатися непоміченою власником хоста.

Активність ботнетів є переважно денною, тому що заражені комп'ютери зазвичай вимкнені вночі.

Географічна відстань між ботами та ботмастером істотно ускладнює відстеження активності останнього правоохоронними органами. Відстань між ботами, які зазвичай знаходяться в різних країнах та сегментах інтернету також ускладнює моніторинг їхнього трафіку та протидію діяльності ботнету.

До появи ботнету Mirai традиційно заражалися переважно системи під управління ОС Windows.

Типова архітектура ботнетів

Архітектура ботнетів класифікується залежно від каналу управління (C&C) і може бути централізованою, децентралізованою або гібридною [1].

Централізована архітектура є різновидом класичної моделі клієнт-сервер. Її типовим прикладом є реалізація управління ботнетом за протоколом IRC. За централізованої моделі C&C кожен бот встановлює комунікаційний канал з одним або декількома серверами управління, які надсилають ботам команди та оновлення шкідливого ПО.

Перевагами централізованої архітектури є швидка реакція та добра координація. Зворотній зв'язок дозволяє ботмастеру зручно моніторити статус ботнета, надаючи інформацію про кількість ботів та їх географічний розподіл.

Головною вадою централізованої архітектури є те, що сервер управління виступає ключовою точкою відмови. Його нейтралізація призводить до руйнування ботнету. Ця слабкість призвела до розвитку децентралізованих архітектур.

Головними протоколами взаємодії у централізованій архітектурі є IRC та HTTP.

У випадку IRC-ботнету ботмастер на сервері управління створює IRC-канали, до яких підключаються комп'ютери-зомбі, чекаючи на команди для виконання шкідливої активності. Така модель все ще лишається досить популярною. Її цікавою рисою є можливість надсилати команди як ботнету в цілому, так і окремим ботам: наприклад, можна обрати групу ботів для виконання атаки. Іншими рисами є надлишковість, масштабованість та різноманітність, які дозволяють багаторазово використовувати програмний код для ботів та збільшувати ботнет.

Істотним недоліком цієї архітектури є легкість виявлення та блокування IRC-трафіку адміністратором мережі. Як

правило в корпоративних мережах він заблокований за замовчуванням.

Через вищевикладене набрала популярності архітектура управління ботнетами через протокол HTTP, який зазвичай дозволений у переважній більшості мереж і добре маскує комунікацію між ботмастером і ботами. Проте цій архітектурі властивий той самий недолік, що й IRC, а саме: наявність в системі центральної точки відмови.

Децентралізована архітектура надає сучасним ботнетам значної гнучкості та стійкості [11]. Нейтралізація навіть значної кількості ботів не означає руйнування всього ботнету, оскільки відсутній центральний сервер управління. Децентралізовані архітерктури реалізуються зазвичай на базі протоколів P2P, наприклад мереж файлообміну.

Гібридна архітектура поєднує риси централізованої та P2P [12]. Типовим прикладом є модель з суперпірами (superpeers), коли боти поділяються на дві групи: клієнти та сервери. Боти-сервери поводяться одночасно як звичайні боти та як сервери управління. Вони мають статичні IP-адреса. Боти-клієнти, в свою чергу, не приймають вхідних підключень, мають динамічні IP-адреси та можуть розміщуватися за брандмауерами. Боти-сервери єдині з ботів мають свої адреси у списку пірів та слухають визначений порт в очікуванні вхідних підключень. Вони також використовують самозгенерований ключ для симетричного шифрування комунікацій, що ускладнює виявлення ботнета. Всі боти-клієнти періодично підключаються до ботів-серверів у своєму списку пірів для отримання команд ботмастера. Коли бот отримує нові команди, які він раніше не спостеріга, він передає їх всім ботам-серверам в своєму списку пірів.

Останнім часом спострерігається зацікавленість ботмастерів у реєстрації серверів управління в домені .bit. Його немає в списку доменів верхнього рівня ICANN. Замість цього він використовує систему Namecoin, побудовану за допомогою технології блокчейн. На відміну від Bitcoin, користувачі розподіленої бази Namecoin мають можливість зберігати в ній дані, зокрема адреси у домені .bit. Відповідні записи бази даних містять IP-адреси, дозволені цим доменом. Даний домен вважається стійким до цензури, оскільки тільки особа, яка зареєструвала ім'я в цьому домені, може змінити відповідні цьому імені IP-адреси. Це означає, що припинити роботу зловмисного сервера при застосуванні цього домена набагато складніше.

Методи виявлення та знешкодження ботнетів

Загальним спостереженням багатьох попередніх досліджень є те, що ботнети являють собою мішені, що постійно рухаються. Всі аспекти життєвого циклу ботнету можуть змінюватися та розвиватися протягом часу. Жодна техніка виявлення або протидії не може бути ефективною постійно.

Активність ботнета проявляється досить швидко після інфільтрації, коли скомпрометована система починає виконувати зловмисні команди. Найбільш поширеними є наступні симптоми:

- з'єднання з серверами управління для отримання команд;
- створення трафіку IRC через асоційовані з цим протоколом порти;
- генерація одночасних та ідентичних запитів до DNS;
- зниження швидкості роботи комп'ютера та доступу до інтернет.

Ці питання виникають як на рівні окремого скомпрометованого хоста так і на рівні локальної мережі. Для послуг мережевого адміністратора існують різноманітні методи та інструменти виявлення ботнетів, що застосовуються на обох рівнях.

На рівні хоста заходи виявлення зазвичай починаються з антивірусного рішення, оскільки інфікування відбувається через встановлення зловмисного ПО. Проте антівірусні технології, що покладаються на

сигнатурне виявлення, самі по собі не можуть ідентифікувати нові варіанти зловмисного ПО, оскільки його сігнатури може ще не бути в базі даних, а отже потрібне ще й евристичне виявлення [13], [14].

Виявлення ботнетів на рівні хоста включає перевірку таких видів активності як встановлення руткітів, несподівані вспливаючі вікна під час веб-серфінгу через HTTP, підозрілі зміни у файлі hosts, які можуть застосовуватися для обмеження доступу до зовнішніх серверів. Якщо було змінено сервери DNS, встановлені за замовчуванням, то це може бути ознакою того, що трафік спрямовується у небажаних напрямках.

Виявлення ботнетів на базі локальної мережі передбачає дещо складніші методи. Перш за все це виявлення IRC-трафіка та спостереження за ним, оскільки зазвичай він не повинен знаходитися у локальній мережі підприємства чи установи. Крім того, IRC-трафік пересилається незашифрованим, отже можлива крадіжка конфіденційної інформації пакетними сніферами. Хоча за замовчанням за протоколом IRC зарезервований порт 6667, боти можуть використовувати діапазон портів 6660-6669 [15].

Коли багато комп'ютерів намагаються одночасно підключитися до однієї або декількох адрес, то це може означати, що з вашої локальної мережі відбувається DDoS-атака. Аналогічно незвичайно великий SMTP-трафік скоріше за все пов'язаний з розсилкою спаму. Засоби мережевої безпеки зазвичай мають гнучкі у налаштовуванні правила для виявлення подібних ознак діяльності ботнету [16].

Існують два різних методичних підходи до виявлення ботнетів: статичний аналіз і біхевіористичний аналіз. Перший є простим та швидким методом, другий – більш детальним да вимогливим до обчислювальних ресурсів.

Статичний аналіз є першою лінією оборони, яка шукає специфічні ознаки діяльності зловмисного ПО на кшталт сигнатур, певних виконуваних файлів, адрес серверів управління ботнетами і т.д. На жаль ефективність статичного аналізу останніми роками постійно знижується, оскільки ботмастери стають більш витонченими у своїх спробах обійти прості методи захисту за допомогою таких засобів як поліморфізм, упаковка та обфускація бінарних файлів, fast-flux DNS і т.п.

Саме тому зростає важливість біхевіористичного аналізу, який моніторить аномальну активність, що і може бути ознакою інфекції. Наприклад часовий розклад активності ботнету може надати багато інформації для аналізу: сервери управління зазвичай розсилають багато однакових команд ботам на виконання певного виду активності, створюючи чималий мережевий трафік в певні моменти часу [17].

Боту потрібно дуже небагато часу, щоб приєднатися до великої кількості серверів, що сильно відрізняється від звичайного паттерну веб-серфінгу користувача. Також для бота з цієї ж причини властива велика кількість невдалих спроб з'єднання, крім того дуже характерно використання IP-адрес замість імен серверів. Сканування портів локальної мережі для пошуку нових можливостей інфільтрації взагалі є класичною поведінкою бота. Всі ці дії можуть бути виявлені шляхом застосування правил сучасних систем виявлення вторгнення (Intusion Detection Systems, IDS).

Децентралізована пірінгова архітектура, яка стала останнім часом популярною у ботмастерів, ускладнює виявлення ботнетів – команди замість серверів управління віддаються пірами, тобто самими ботами. Проте інфіковані ботами комп'ютери завжди діють аналогічно тому, як би вони діяли за централізованої архітектури, оскільки ботмастер має ту саму мету.

На щастя з розвитком ботнетів розвивалися й засоби їх виявлення та знешкодження. Сучасні методи концентруються головним чином на виявленні та швидкому реагуванні, в той час як прогнозуванню атак приділяється

порівняно мало уваги. На сьогодні методи розділяються на три групи:

- ті, що можуть ідентифікувати конкретну атаку, але не можуть її передбачити заздалегідь;
- ті, що мають прогнозну спроможність, але обмежені конкретними видами атак;
- ті, що можуть прогнозувати інфікування ботнетом, але не в змозі передбачити поведінку ботнета після інфікування.

Такі недоліки роблять доцільним побудову системи, здатної прогнозувати конкретні біхевіористичні етапи потенційно інфікованих комп'ютерів, лишаючись незалежними від типів атак або ботнетів.

Перспективним є підхід на основі марковських ланцюгів. Ботнети виявляють зловмисну поведінку, відмінну від просто атак. Інфікування часто-густо починається з атак соціальної інженерії або експлуатоції хоста-жертви, призводячи до завантаження зловмисного бінарного файла. Якщо останній буде виконано, то це може викликати участь у атаці, комунікацію з сервером управління або завантаження подальших оновлень ботнету. Виходячи з того, що атаки відбуваються в такому контексті, то можливе моделювання поведінкових етапів інфікованого комп'ютера до та після того, як він візьме участь у атаці [18]. Коли така модель побудована, вона може використовуватися для прогнозування часу початку атаки виходячи з поведінкової послідовності інфікованого хоста, дозволяючи генерувати ранні попередження про атаку.

Із розповсюдженням смартфонів та планшетів особливої привабливості для зловмисників набувають ботнети з мобільних пристроїв. Аналогічно до традиційних мобільні ботнети здатні брати участь у тих самих видах кримінальної активності. В операційних системах та іншому ПО мобільних пристроїв постійно знаходять нові вразливості, що робить цей вид устаткування потенційною мішенню для набуття незаконного доступу та подальшою участі у звичайних для ботнетів видах зловмисної активності. Нова система SMARTbot для виявлення ботнетів з пристроїв на базі операційної системи Android побудована за допомогою технологій машинного навчання [19]. Складається вона з трьох модулів: динамічного аналізу, знаходження характерних рис та навчання. Під час динамічного аналізу підозрілі програми виконуються у безпечній «пісочниці» та збираються для подальшої класифікації. Під час знаходження характерних рис екстрагується вектор останніх та генеруються профілі програм. Кінець-кінцем у модулі навчання дані про відомі ботнети застосовуються для тренування нейронної мережі.

Для протидії ботнетам з децентралізованою архітектурою пропонується система розпізнавання краулерів BoobyTrap [20], що дозволяє автоматично виявляти активність краулерів у P2P-мережах.

Он-лайнові соціальні мережі (online social network, OSN) останнім часом піддаються постійно зростаючому впливу соціальних ботів [21], які є програмно контрольованими обліковими записами, що копіюють людську поведінку зі зловмисними намірами. За оцінками Bloomberg не менше 40 % облікових записів у Facebook, Twitter та інших популярних OSN належить спамерам (соціальним ботам) [22]. Соціальним ботнетом зазвичай називають групу соціальних ботів під контролем єдиного ботмастера, який здійснює зловмисну активність, імітуючи взаємодію між нормальними користувачами OSN для зниження ризику виявлення. Наприклад, соціальні боти у Твіттері можуть бути «фоловерами» інших аккаунтів, ретвітувати твіти або відповідати на них. Оскільки зміщена величина following/follower ratio є типовою рисою соціального бота, то підтримуючи цю величину на збалансованому рівні, індивідуальним ботам легше запобігти виявленню. Створення соціального ботнета є доволі легкою справою через відкриті API

соцмережі. Незважаючі на численні повідомлення про існування соціальних ботнетів [23], [24] адміністрація соціальних мереж не вважає за потрібне вживати якихось істотних обмежуючих заходів.

Головною метою створення соціальних ботнетів є розсилка спаму, торгівля фоловерами, поширення дезінформації та політична агітація (пропаганда). Традиційно адміністрація Twitter блокує лише обліковий запис, з якого виходить оригінальне спам-повідомлення, а боти, які роблять ретвіт, лишаються неушкодженими. Для боротьби з соціальними ботнетами пропонується для кожного облікового запису запровадити статистику ретвітів (репостів) спаму або дезинформації. Облікові записи, для яких така статистика перевищує деякий поріг, підлягають блокуванню.

Висновки

Ботнетам присвячена велика кількість сучасних досліджень, проте ефективність методів їх виявлення та знешкодження все ще лишається суперечливою. Метою даної статті є ідентифікація цієї серйозної проблеми інформаційної безпеки, оцінка дієвості отриманих результатів та надання рекомендацій щодо їх пруденційного використання.

Ботнети відіграють провідну роль у створенні загроз інформаційній безпеці сучасного інтернету, породжуючи 80 % спаму. Зловмисники контролюють армії ботів, здійснюючи незаконну діяльність у вигляді DDoS-атак, клік-фроду, майнінгу криптовалют і т.д.

Першим необхідним кроком на шляху запобігання ботнетам є запровадження ефективної техніки виявлення у вигляді системи виявлення вторгнення (IDS), яка може бути статичною (сигнатурною) та динамічною (поведінковою). Більшість наукових робіт розглядають саме системи останнього типу.

Після виявлення ботнетів наступним кроком стає визначення шляхів знищення інфраструктури ботнета та його знешкодження. Найбільш вживаними методами є порушення каналів управління та перешкоджання ботмастерові у надсиланні команд ботнету.

В свою чергу, з боку ботмастерів продовжують швидко розвиватися техніки запобігання виявленню. Останніми кроками є міграція ботнетів на нові платформи, включаючи мобільні пристрої та IoT. Іншим трендом є поява міні-ботнетів, які спеціалізуються переважно на крадіжках інформації замість DDoS-атак і через свої відносно невеликі розміри є досить важкими у виявленні.

Одним з головних питань для дослідників лишається складність тестування їхніх пропозицій у реальних умовах з реальними даними.

Через глобальний характер ботнетів критичної важливості набуває питання кооперації між дослідниками, приватними установами та правоохоронними органами різних країн у боротьбі з ботнетами. Головним викликом є розробка глобальної, розподіленої та кооперативної системи виявлення та знешкодження ботнетів. Також важливим є обговорення міжнародних правових питань та питань наднаціональної політики у боротьбі із загрозою ботнетів.

References

[1] S. S. C. Silva, R. M. P. Silva, R. C. G. Pinto, and R. M. Salles, “Botnets: A survey,” Comput. Netw., vol. 57, no. 2, pp. 378–403, Feb. 2013.

[2] “Operation Tovar,” Wikipedia. 16-Jan-2017.

[3] “Eggdrop,” Wikipedia. 27-Oct-2016.

[4] “WORM_SDBOT.AZ - Threat Encyclopedia - Trend Micro US.” [Online]. Available: https://www.trendmicro.com/vinfo/us/threat-encyclopedia/archive/malware/worm_sdbot.az. [Accessed: 18-Feb-2017].

[5] “WORM_AGOBOT.XE - Threat Encyclopedia - Trend Micro US.” [Online]. Available: https://www.trendmicro.com/vinfo/us/threat-encyclopedia/archive/malware/worm_agobot.xe. [Accessed: 18-Feb-2017].

[6] J. B. Grizzard, V. Sharma, C. Nunnery, B. B. Kang, and D. Dagon, “Peer-to- peer botnets: overview and case study,” in Proceedings of the First Conference on First

Workshop on Hot Topics in Understanding Botnets, Berkeley, CA, USA, 2007, pp. 1–8.
[7] D. Lawrence, “The Hunt for the Financial Industry’s Most-Wanted Hacker - Bloomberg,” 18-Jun-2016. [Online]. Available: https://www.bloomberg.com/news/features/2015-06-18/the-hunt-for-the-financial-industry-s-most-wanted-hacker. [Accessed: 24-Feb-2017].
[8] “Mirai (malware),” Wikipedia. 18-Feb-2017.
[9] “GitHub - James-Gallagher/Mirai: Source code for the Mirai botnet - Not going anywhere anytime soon.” [Online]. Available: https://github.com/James-Gallagher/Mirai. [Accessed: 20-Feb-2017].
[10] “Biggest-ever DDoS attack takes down high-profile web services,” Comput. Fraud Secur., vol. 2016, no. 11, pp. 1–3, Nov. 2016.
[11] Q. Han, W. Yu, Y. Zhang, and Z. Zhao, “Modeling and evaluating of typical advanced peer-to-peer botnet,” Perform. Eval., vol. 72, pp. 1–15, Feb. 2014.
[12] S. Heron, “Botnet command and control techniques,” Netw. Secur., vol. 2007, no. 4, pp. 13–16, Apr. 2007.
[13] A. C. Atluri and V. Tran, “Botnets Threat Analysis and Detection,” in Information Security Practices, I. Traoré, A. Awad, and I. Woungang, Eds. Springer International Publishing, 2017, pp. 7–28.
[14] “Heuristic botnet detection,” 24-May-2011.
[15] C.-M. Chen and H.-C. Lin, “Detecting botnet by anomalous traffic,” J. Inf. Secur. Appl., vol. 21, pp. 42–51, Apr. 2015.
[16] A. K. Seewald and W. N. Gansterer, “On the detection and identification of botnets,” Comput. Secur., vol. 29, no. 1, pp. 45–58, Feb. 2010.
[17] J. Ersson and E. Moradian, “Botnet Detection with Event-Driven Analysis,” Procedia Comput. Sci., vol. 22, pp. 662–671, 2013.
[18] Z. Abaid, D. Sarkar, M. A. Kaafar, and S. Jha, “The Early Bird Gets the Botnet: A Markov Chain Based Early Warning System for Botnet Attacks,” in 2016 IEEE 41st Conference on Local Computer Networks (LCN), 2016, pp. 61–68.
[19] A. Karim, R. Salleh, and M. K. Khan, “SMARTbot: A Behavioral Analysis Framework Augmented with Machine Learning to Identify Mobile Botnet Applications,” PLOS ONE, vol. 11, no. 3, p. e0150077, Mar. 2016.
[20] S. Karuppayah, E. Vasilomanolakis, S. Haas, M. Mühlhäuser, and M. Fischer, “BoobyTrap: On autonomously detecting and characterizing crawlers in P2P botnets,” in 2016 IEEE International Conference on Communications (ICC), 2016, pp. 1–7.
[21] E. Ferrara, O. Varol, C. Davis, F. Menczer, and A. Flammini, “The Rise of Social Bots,” Commun ACM, vol. 59, no. 7, pp. 96–104, Jun. 2016.
[22] “‘Likejacking’: Spammers Hit Social Media - Bloomberg.” [Online]. Available: https://www.bloomberg.com/news/articles/2012-05-24/likejacking-spammers-hit-social-media. [Accessed: 26-Feb-2017].
[23] Y. Boshmaf, I. Muslukhov, K. Beznosov, and M. Ripeanu, “Design and analysis of a social botnet,” Botnet Act. Anal. Detect. Shutdown, vol. 57, no. 2, pp. 556–578, Feb. 2013.
[24] G. Yan, “Peri-Watchdog: Hunting for hidden botnets in the periphery of online social networks,” Comput. Netw., vol. 57, no. 2, pp. 540–555, Feb. 2013.

Реферат

Сігайов Андрій; Воловик Андрій

Ботнети: методи виявлення та протидії

Через свої практично необмежені розміри та можливості ботнети складають одну з найбільш серйозних загроз інформаційній безпеці. Найбільш небезпечними властивостями ботнетів є здатність діяти приховано протягом тривалого часу, їхні розміри та важкість їхнього виявлення. Метою даної статті є ідентифікація цієї серйозної проблеми інформаційної безпеки, оцінити дієвість отриманих результатів та надати рекомендації щодо їх раціонального використання. Першим необхідним кроком на шляху запобігання ботнетам є запровадження ефективної техніки виявлення у вигляді системи виявлення вторгнення, яка може бути статичною (сигнатурною) та динамічною (поведінковою). Після виявлення ботнету наступним кроком стає визначення шляхів знищення інфраструктури ботнета та його знешкодження. Найбільш вживаними методами є порушення каналів управління та перешкоджання ботмастерові у надсиланні команд ботнету.

Сучасні методи концентруються головним чином на виявленні та швидкому реагуванні, в той час як прогнозуванню атак приділяється

порівняно мало уваги. Перспективним є підхід на основі марковських ланцюгів.

Сигаёв Андрей; Воловик Андрей

Ботнеты: методы обнаружения и противодействия

Из-за своих практически неограниченных размеров и возможностей ботнеты составляют одну из самых серьезных угроз информационной безопасности. Наиболее опасными свойствами ботнетов является способность действовать скрытно в течение длительного времени и трудность их обнаружения. Целями данной статьи являются идентификация этой серьезной проблемы информационной безопасности, оценка эффективности полученных результатов и предоставление рекомендаций по их рациональному использованию. Первым необходимым шагом на пути обезвреживания ботнета является внедрение эффективной техники обнаружения в виде системы обнаружения вторжения, которая может быть статической (сигнатурной) или динамической (поведенческой). После обнаружения ботнета следующим шагом является определение путей уничтожения инфраструктуры ботнета и его обезвреживания. Наиболее распространёнными методами являются нарушение каналов управления и препятствование ботмастеру в передаче команд ботнета.

Современные методы концентрируются главным образом на выявлении и быстром реагировании, в то время как прогнозированию атак уделяется сравнительно мало внимания. Перспективным представляется подход на основе марковских цепей.

Sigayov Andriy; Volovyk Andriy

Botnets: detection and counteraction methods

Through its almost unlimited size and possibilities botnets are one of the most serious threats to information security. The most dangerous botnets features are the ability to operate secretly for a long time, their size and difficulty of their detection. The purpose of this paper is to identify this serious problem of information security, evaluate the validity of the results and provide recommendations for their rational use. The first necessary step towards preventing botnets is the introduction of effective detection techniques as intrusion detection systems, which can be static (signature based) and dynamic (behavioral). After botnet dietection, the next step is to identify ways of botnet infrastructure destruction and its neutralization. The most common methods are to break the control channels and to obstruct botmaster in sending botnet command.

Modern methods focus mainly on detection and rapid response, while forecasting of attacks is given relatively little attention. A promising approach seems to be based on Markov chains.

Відомості про авторів

Сігайов Андрій Олександрович

Освіта: Повна вища, «Програмне забезпечення обчислювальної техніки та автоматизованих систем» (1995).

Науковий ступінь: Доктор економічних наук (2004).

Вчене звання: Професор (2008).

Місце роботи: Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського».

Область знань: Економіка, інформаційні технології.

Наукові інтереси: Фінанси, математичне моделювання, інформаційна безпека.

Email: *a.sigayov@kpi.ua*

Воловик Андрій Вікторович

Освіта: Повна вища, «Економічна кібернетика» (2005).

Місце роботи: Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського».

Область знань: Економіка, інформаційні технології.

Наукові інтереси: Економіка охорони здоров'я, системи підтримки ухвалення рішень, інформаційна безпека.

Email: *andrew.volovyk@gmail.com*

УДК 629.039

ЗАЩИТА ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ ОТ РАДИОАКТИВНОГО И ХИМИЧЕСКОГО ЗАГРЯЗНЕНИЯ АТМОСФЕРЫ

Гончаренко Юлия; Качур Тарас; Мирошник Олег; Рыжкин Алексей
Государственное учреждение «Институт геохимии окружающей среды НАН Украины»

PROTECTION OF OBJECTS OF CRITICAL INFRASTRUCTURE FROM RADIOACTIVE AND CHEMICAL POLLUTION OF THE ATMOSPHERE

Goncharenko Julia; Kachur Taras; Miroshnik Oleg; Ryzhkin Alexei
State Institution «Institute of Environmental Geochemistry of NASU»

Анотація: **Розглядається новий концептуальний підхід щодо організації захисту об'єктів критичної інфраструктури від радіоактивних і хімічних забруднень атмосфери. Він передбачає створення спеціальних захисних комунікацій на базі конференц-залів, їдалень, кафе, які повсякденно використовуються за прямим призначенням.**
Ключові слова: **Об'єкт критичної інфраструктури, радіоактивне забруднення, хімічне забруднення, фільтровентиляційна установка.**
Summary: **A new conceptual approach is being considered to organize the protection of critical infrastructure facilities from radioactive and chemical pollution of the atmosphere. It provides for the creation of special security communications on the basis of conference halls, canteens, cafes, which continue to be used on a daily basis for their intended purpose.**
Keywords: **Critical Infrastructure Object, radioactive contamination, chemical pollution, filter-ventilation installation.**

Введение

К объектам критической инфраструктуры относятся атомные, тепловые и гидроэлектростанции, химические и нефтехимические комбинаты, металлургические заводы и предприятия оборонной промышленности, телекоммуникационные центры (узлы связи) и множество других государственных предприятий и частных учреждений, выход из строя или нарушение функционирования которых может вызвать потерю управления или привести к существенным потерям на общегосударственном, региональном или местном уровне [1] – [3]. Защита критической инфраструктуры является важной проблемой для всех стран. Основные мероприятия по защите направлены, как правило, на снижение уровня уязвимости объектов критической инфраструктуры по отношению к природным явлениям и авариям, к террористическим актам и другим преступным деяниям [4] – [7].

Последние десятилетия Украина остается страной техногенных аварий и катастроф [8], [9], которые сопровождаются загрязнением атмосферы и распространением опасных и токсичных химических соединений. Пожары, происходящие в Чернобыльской зоне и других «мертвых» лесных массивах, приводят не только к химическому, но и к радиоактивному загрязнению воздушной среды.

Как показывает мировой опыт, в качестве грязных бомб террористы могут использовать радиоактивные и отравляющие вещества, которые взрывной волной распыляются в атмосфере и ветром разносятся на большие расстояния [10] – [12]. С этой точки зрения защита объектов критической инфраструктуры сужается до защиты персонала от поражения токсичными и радиоактивными веществами, распыленными в атмосфере. В

этом случае отсутствует поражающее действие ударной волны, как это происходит при применении ядерного оружия, поэтому для защиты персонала не обязательно создавать специальные защитные сооружения, способные выдерживать поражающие факторы ядерного взрыва, как это было в годы холодной войны. В связи со сказанным выше, необходимо разрабатывать новые концептуальные подходы для коллективных средств защиты персонала объектов критической инфраструктуры.

Для решения этой актуальной научной задачи проанализируем поражающие факторы радиоактивного и химического загрязнения атмосферы, рассмотрим состояние существующих защитных сооружений, сформулируем новые концептуальные подходы для коллективных средств защиты персонала объектов критической инфраструктуры.

Поражающие факторы радиоактивного и химического загрязнения атмосферы

Растущая опасность испытательных ядерных взрывов была осознана достаточно давно. К середине 60-х годов стало ясно, что их продолжение, по крайней мере, в воздухе, на земле и на воде скоро приведет к такому повышению уровня радиации на всей Земле, который не только вызовет невиданный рост количества раковых заболеваний, но и необратимо разрушит генофонд человечества, чем обречет его на вырождение. Именно это заставило ведущие ядерные державы, несмотря на острое военное и политическое противостояние «Запада» и «Востока», заключить договор о запрете ядерных испытаний в воздухе, на земле и на воде. Подземные ядерные испытания с 2012 года также полностью прекращены.

Но источники поступления радиоактивных загрязнений в атмосферу, как и в другие среды, не ограничиваются ядерными взрывами. Промышленное производство обогащенного урана для атомных бомб и ядерных реакторов, переработка плутония, получаемого в реакторах, производство радиоизотопов для промышленных и исследовательских целей постоянно создают угрозу утечки в окружающую среду какой-то части радиоактивных материалов. Особенно велика такая опасность при транспортировке, переработке и захоронении радиоактивных отходов атомных электростанций.

Образующиеся в ходе этих процессов радиоактивные отходы можно подразделить на два типа: продукты деления, которые содержатся в общей массе первичного и вторичного топлива, и внешние активированные продукты, находящиеся, главным образом, в охлаждающих средах.

Первичные загрязнения вызваны радиоактивными веществами, которые образовались в процессе аварии, производственной деятельности, взрывов ядерных боеприпасов. Вторичные радиоактивные загрязнения определяются переходом радиоактивности с загрязненных объектов на чистые. Радионуклиды с загрязненных сооружений, транспорта и дорог могут переходить обратно в воздушную среду, а затем оседать, загрязнять незагрязненные, а также уже грязные объекты. Один и тот же объект может за счет вторичных процессов загрязняться несколько раз. В этих условиях вторичные загрязнения становятся многократными. Наиболее опасными источниками загрязнения являются выбросы радиоактивных веществ в атмосферу и их распространение в виде аэрозольного облака.

Радиоактивное загрязнение атмосферы может произойти в результате террористического акта. Здесь рассматривается два основных сценария. В первом случае это использование ядерных боеприпасов, разрушение ядерных объектов, радиационное заражение местности и поражение людей. Во втором – использование грязных радиоактивных бомб.

Наиболее распространенные группы загрязнителей воздуха: атмосферные газы

(окислы азота, серы, углерода, например, углекислый газ), углеводороды, фенолы, аэрозоли тяжелых металлов и другие органические и минеральные соединения.

Аэрозоли – взвешенные в газообразной среде частички твердых или жидких веществ как органического, так и неорганического происхождения. Они могут содержать сложные комплексы химических веществ, в том числе обладающих высокой степенью токсичности и представляющих опасность для здоровья человека. Наиболее значительный источник загрязнения воздуха – автотранспорт, поставляющий в атмосферу свинец, окись углерода и полициклические ароматические углеводороды, среди которых наиболее опасны бензапирен и фенантрен.

Значительную долю загрязнения воздуха составляют также выбросы тепловых электростанций и предприятий химической промышленности, которые выбрасывают в атмосферу углеводороды, фенолы, органические фториды и хлориды, карбоновые кислоты, альдегиды, органические соединения серы, хлора, фтора, азота, двуокись серы, сероводород, окислы азота, соляную кислоту и другие кислоты.

Попадание вредных веществ в атмосферу может происходить не только в результате техногенных аварий, катастроф и пожаров, но и в результате террористического акта с использованием грязных бактериологических бомб, путем загрязнения водоемов и систем водообеспечения с целью уничтожения или вывода из строя населения.

Таким образом, поражающими факторами радиоактивного загрязнения атмосферы являются радиоактивные частицы, как результат первичного деления ядерного материала, радиоактивные частицы, являющиеся результатом вторичного облучения, радиоактивные газы и аэрозоли, а также радионуклиды, образующиеся при активации ядер воздуха. Поражающими факторами химического загрязнения атмосферы являются окислы, фенолы, углеводороды, а также аэрозоли различных химических, в том числе и высокотоксичных веществ, а также продукты разложения и горения. Они попадают и образуются в атмосфере в результате ядерных взрывов, техногенных аварий, пожаров техногенных и природных объектов, а также взрывов грязных радиоактивных и химических бомб.

Состояние существующих защитных сооружений

В Украине имеется достаточно большое количество инженерных сооружений, предназначенных для защиты населения и военнослужащих от поражающих факторов оружия массового поражения, которые строились систематически по особому плану и представляют собой, как правило, сооружения или отдельные, или встроенные в подвальную часть зданий. Они рассчитывались на длительный срок эксплуатации.

Это сложные в техническом отношении сооружения, которые обеспечивали требуемые нормативные условия жизнеобеспечения людей в течение расчетного времени. Они создавали надежную защиту людей от ударной волны, светового излучения, проникающей радиации и радиоактивного заражения при ядерных взрывах, от отравляющих веществ и бактериальных средств, а также от высоких температур и вредных газов в зоне пожаров и оборудовались системами вентиляции, водоснабжения, канализации, отопления, освещения и средствами телекоммуникаций.

К сожалению, большая часть защитных сооружений после девяностых годов использовалась под складские помещения и даже под овощехранилища, в результате чего они пришли в состояние, которое не позволяет их использовать по прямому назначению Некоторые из них находятся в удовлетворительном и даже хорошем состоянии. Однако оборудование и физически, и морально устарело.

Кроме этого, работающий там персонал, как правило, не имеет специальной

подготовки и не в состоянии обслуживать (выполнять периодические регламенты) оборудование, установленное в защитных сооружениях, и тем самых обеспечить их боевую готовность для рения задач при возникновении различных чрезвычайных ситуаций.

Приведенные выше сведения о состоянии существующих защитных сооружений свидетельствуют об острой необходимости в разработке новых концептуальных подходов к созданию коллективных средств защиты персонала объектов критической инфраструктуры.

Новые концептуальные подходы к созданию коллективных средств защиты персонала объектов критической инфраструктуры

Новый концептуальный подход к проблеме защиты персонала объектов критической инфраструктуры состоит в следующем. Поскольку основным поражающим фактором является распыление в воздухе радиоактивных и токсичных веществ и аэрозолей, которые воздействуют на органы дыхания и кожные покровы, то в первую очередь их и надо защищать. Используемые на АЭС и химических производствах изолирующая спецодежда и противогазы различных модификаций не могут быть внедрены на всех объектах критической инфраструктуры, как минимум, по трем причинам. Во-первых, средства защиты должны быть индивидуальными, то есть подогнанными персонально под каждого работника. Во-вторых, необходимо как минимум 2 раза в неделю проводить тренировки по их использованию для поддержания элементарных навыков. В-третьих, эти средства должны проходить ежегодную поверку соответствующими компетентными службами, что является достаточно затратным и хлопотным мероприятием.

Как альтернатива предлагается на объектах критической инфраструктуры размещать специальные защитные конструкции, которые позволят в случае радиационной и химической опасности защитить большие группы людей, в первую очередь, административный персонал. Для этих целей могут быть использованы помещения, специально предназначенные для сбора большого количества людей, например, залы для совещаний, конференц-залы, столовые, кафе и т. п. Они оборудуются специальными фильтровентиляционными установками, которые обеспечивают очистку и циркуляцию воздуха, подаваемого в защитное помещение, и создают подпор, не позволяющий опасным веществам попадать в помещение и поражать персонал. Даже если подпор в подобных помещениях создать не удается, то, как показывают многочисленные эксперименты, отток воздуха через негерметичности защитного помещения не позволяет вредным веществам проникать в него.

В организации такого рода защитных конструкций есть 2 положительных фактора. Во-первых, при проверке работоспособности фильтровентиляционных установок не требуется большого числа дополнительных сотрудников. Во-вторых, у персонала объекта появляется уверенность, что они всегда защищены от возможных неожиданностей. Тем более, что время пребывания в защитных помещениях определяется временем прохождения облака радиоактивных или отравляющих веществ в контролируемой зоне.

Очевидно, что создание подобных защитных помещений многократно дешевле специальных укрытий, но достаточно дорог, поэтому предлагается второй вариант защиты персонала – это переносная инженерная конструкция. В ее основу положена быстро развертывающаяся палатка и встроенная в нее фильтровентиляционная установка, работающая от бытовой электросети как обычный электроприбор. Палатка разворачивается после включения фильтровентиляционной установки. Благодаря двойным липучим застежкам вход герметизируется. Сидя на полу в ней

может разместиться от 10 до 40 человек в зависимости от конкретного конструкторского исполнения. Компактно уложенные, такие средства коллективной защиты могут располагаться рядом с пожарными точками в коридорах, на лестничных площадках и в других предусмотренных для этого местах.

Недостатком и первого, и второго типа укрытий является их зависимость от электросети, поэтому предлагается третий тип коллективного средства защиты – малогабаритная палатка, в которой может разместиться сидя 4-5 человек. Двойная липучая застежка обеспечивает герметизацию входа. Условный подпор создается вытравливанием сжатого воздуха (кислорода) из баллона через специальный редуктор.

Выводы

Новый концептуальный подход в защите объектов критической инфраструктуры от радиоактивных и химических загрязнений атмосферы состоит в создании новых коллективных средств защиты, которые предназначены для защиты органов дыхания и кожных покровов персонала. Их конструкторское исполнение предусматривает создание специальных защитных помещений на базе конференц-залов, столовых, кафе, которые продолжают повседневно использовать по прямому назначению посредством оснащения их стационарными фильтровентиляционными установками, обеспечивающими в них подпор воздуха при укрытии людей.

Переносные коллективные средства защиты создаются на базе надувных палаток, сделанных из специальных изолирующих материалов, подпор воздуха в которых создается вмонтированной фильтровентиляционной установкой или вытравливанием сжатого воздуха (кислорода) из баллона через специальный редуктор.

Перелік посилань

[1] *Указ Президента України №8/2017 від 16 січня 2017 року.* Доступ: http://www.president.gov.ua/documents/82017-21058

[2] *Critical infrastructure – content, structure and problems of its protection.* Input: https://www.google.com.ua/?gfe_rd=cr&ei=gVWAWMT9FNKBYOfZnOAE&gws

[3] Л. Хофрейтер, *Критическая инфраструктура – содержание, структура и проблемы ее защиты.* Доступ: http:/jml2012.indexcopernicus.com/fulltxt.php?ICID=1129729

[4] Ю. Ю. Гончаренко, *Структура контура управления информационной безопасностью предприятия* / Ю. Ю. Гончаренко // Научно-практический журнал «Экономика и управление». – №5. – Симферополь: НАПКС, 2012. – С. 97 – 101.

[5] Е. В. Азаренко, *Хронология чрезвычайных ситуаций и основные этапы их развития* / Е. В. Азаренко, О. В. Бляшенко, Ю. Ю. Гончаренко, М. М. Дивизинюк // Техногенно-экологическая безопасность и гражданская защита. – Киев: ГП «Институт геохимии окружающей среды НАНУ», 2014. – Вып.7. – С. 119 – 128.

[6] Е. В. Азаренко, *Защита информации в системах мониторинга чрезвычайных ситуаций* / Е. В. Азаренко, О. В. Бляшенко, М. М. Дивизинюк, В. Е. Ковач // Науково-технічний збірник «Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні». – Київ: Державна служба спеціального звуку та захисту інформації в Україні НТУУ «КПІ». – 2015. – Вип. 1. (29). – С. 82 – 87.

[7] С. В. Лазаренко, *Некоторые аспекты безопасности критической инфраструктуры государства* / Ю. Ю. Гончаренко, М. М. Дивизинюк, Н. В. Касаткина, Г. В. Камышенцев, С. В. Лазаренко // Інформаційна безпека – науковий журнал східноукраїнського національного університету імені Володимира Даля. Северодонецьк: СУНУ ім. В. Даля. – №4(24). – 2016. – С. 135 – 140.

[8] *Загрязнения атмосферного воздуха.* Доступ: http://eco1ogy-education.ru/index.php?action = full&id=517

[9] *Загрязнение атмосферы радиоактивными веществами* Доступ: http://www.saveplanet.su/articles_7.html

[10] Ю. Ю. Гончаренко, *Математическая модель выявления низкоактивного ионизирующего гамма-излучения* / Ю. Ю. Гончаренко, М. М. Дивизинюк, А. В. Фаррахов // Наука та техніка Повітряних сил Збройних сил України. – Харків: ХУПС ім. Кожедуба, 2014. – № 4 (17). – С. 100 – 103.

[11] О. В. Фаррахов, *Потенційні джерела загроз ядерно-радіаційної безпеки. Ядерний тероризм.* / О. В. Фаррахов // Техногенно-екологічна безпека та цивільний захист. – 2015. – № 8. – С. 32 – 40.

[12] В. А. Ліпкан, *Боротьба з тероризмом* / В. А. Ліпкан, Д. І. Никифорчук, М. М. Руденко: Монографічне дослідження. – К.: Знання України, 2002. – 254 с.

References

[1] *Decree of the President of Ukraine No. 8/2017 dated 16 December 2017.* Access: http://www.president.gov.ua/documents/82017-21058

[2] *Critical infrastructure - content, structure and problems of its protection.* Input: https://www.google.com.ua/?gfe_rd=cr&ei=gVWAWMT9FNKBYOfZnOAE&gws

[3] L. Hofreiter. *Critical infrastructure - the content, structure and problems of its protection.* Access: http: /jml2012.indexcopernicus.com/fulltxt.php? ICID = 1129729

[4] Yu. Yu. Goncharenko, *Structure of the information security management contour of the enterprise* / Yu. Yu. Goncharenko // Scientific and Practical Journal "Economics and Management". - №5. - Simferopol: NAPKS, 2012. - P. 97 - 101.

[5] E. V. Azarenko, *Chronology of emergency situations and the main stages of their development* / E. V. Azarenko, O. V. Blyashenko, Yu. Yu. Goncharenko, M. M. Divizinyuk // Technogenic and ecological safety and civil protection. - Kiev: SE "Institute of Geochemistry of the Environment of NASU", 2014. - Issue 7. - P. 119-128.

[6] *Information security in emergency monitoring systems* / E. V. Azarenko, O. V. Blyashenko, M. M. Divizinyuk, V. E. Kovacs // Scientific and technical collection "The legal, regulatory and metrological support of information security in Ukraine" - Kyiv, State Service special sound and Information Protection of Ukraine NTU "KPI", 2015 - Issue 1 (29). - P. 82-87.

[7] S. V. Lazarenko, *Some Aspects of Security of the State's Critical Infrastructure* / Yu. Yu. Goncharenko, M. M. Divizinyuk, N. V. Kasatkina, G. V. Kamyshentsev, S. V. Lazarenko // Information Security - scientific journal East Ukrainian National University of Vladimir Dal. Severodonetsk: Suyu them. Dal, №4 (24) 2016 - P. 135 - 140.

[8] *Pollution of atmospheric air.* Access: http: //eco1ory-education.ru/index.php? Atiоп = full & id = 517

[9] *Pollution of the atmosphere by radioactive substances* Access: http://www.saveplanet.su/articles_7.html

[10] Yu. Yu. Goncharenko, *Mathematical Model for Detection of Low-Level Ionizing Gamma Radiation* / Yu. Yu. Goncharenko, M. M. Divizinyuk, A. V. Farrakhov // Science and Technology of the Air Force of Ukraine. - Kharkov: Hoopes them. Kozhedub, 2014. - № 4 (17) - p. 100-103

[11] A. Farrahov, *Potential sources of threats to nuclear radiation safety. Nuclear terrorism.* / O. V. Farrahov // Technogenic and ecological safety and civil protection. - 2015. - № 8. - P. 32-40.

[12] V. A. .Lipkan, *Combating terrorism* / V. A. Lipkan, D. I. Nykyforchuk, N. M. Rudenko: monographs. - K .: Knowledge Ukraine, 2002. - 254 p.

Реферат

Гончаренко Юлія; Качур Тарас; Мирошник Олег; Рижкін Олексій

Захист об'єктів критичної інфраструктури від радіоактивного та хімічного забруднення атмосфери

У роботі пропонується новий концептуальний підхід до проблеми захисту персоналу об'єктів критичної інфраструктури. Показано, що вражаючими чинниками радіоактивного забруднення атмосфери є радіоактивні частинки як результат первинного розподілу ядерного матеріалу, радіоактивні частинки, які є результатом вторинного опромінення, радіоактивні гази і аерозолі, а також радіонукліди, що утворюються при активації ядер повітря. Вражаючими факторами хімічного забруднення атмосфери є оксиди, феноли, вуглеводні, а також аерозолі різних хімічних, в тому числі і високотоксичних речовин, а також продукти розкладання і горіння. Вони потрапляють і утворюються в атмосфері в результаті ядерних вибухів, техногенних аварій, пожеж техногенних і природних об'єктів, а також вибухів брудних радіоактивних і хімічних бомб.

Велика частина захисних споруд після дев'яностих років використовувалася під складські приміщення та навіть під овочесховища, в результаті чого вони прийшли в стан, який не дозволяє їх

використовувати за призначенням, для якого вони призначалися. Деякі з них знаходяться в задовільному і навіть хорошому стані. Однак обладнання і фізично, і морально застаріло.

Новий концептуальний підхід в захисті об'єктів критичної інфраструктури від радіоактивних і хімічних забруднень атмосфери полягає в створенні нових колективних засобів захисту, які призначені для захисту органів дихання та шкірних покривів персоналу. Їх конструкторське виконання передбачає створення спеціальних захисних приміщень на базі конференц-залів, їдалень, кафе, які продовжують повсякденно використовувати за прямим призначенням за допомогою оснащення їх стаціонарними фильтровентиляционной установками, що забезпечують в них підпір повітря при укритті людей. Переносні колективні засоби захисту створюються на базі надувних наметів, зроблених зі спеціальних ізолюючих матеріалів, підпір повітря в яких створюється вмонтованою фільтровентиляційною установкою або витравлювання стисненого повітря (кисню) з балона через спеціальний редуктор.

Гончаренко Юлия; Качур Тарас;
Мирошник Олег; Рыжкин Алексей

Защита объектов критической инфраструктуры от радиоактивного и химического загрязнения атмосферы

В работе предлагается новый концептуальный подход к проблеме защиты персонала объектов критической инфраструктуры. Показано, что поражающими факторами радиоактивного загрязнения атмосферы являются радиоактивные частицы как результат первичного деления ядерного материала, радиоактивные частицы, являющиеся результатом вторичного облучения, радиоактивные газы и аэрозоли, а также радионуклиды, образующиеся при активации ядер воздуха. Поражающими факторами химического загрязнения атмосферы являются окислы, фенолы, углеводороды, а также аэрозоли различных химических, в том числе и высокотоксичных веществ, а также продукты разложения и горения. Они попадают и образуются в атмосфере в результате ядерных взрывов, техногенных аварий, пожаров техногенных и природных объектов, а также взрывов грязных радиоактивных и химических бомб.

Большая часть защитных сооружений после девяностых годов использовалась под складские помещения и даже под овощехранилища, в результате чего они пришли в состояние, которое не позволяет их использовать по назначению, для которого они предназначались. Некоторые из них находятся в удовлетворительном и даже хорошем состоянии. Однако оборудование и физически, и морально устарело.

Новый концептуальный подход в защите объектов критической инфраструктуры от радиоактивных и химических загрязнений атмосферы состоит в создании новых коллективных средств защиты, которые предназначены для защиты органов дыхания и кожных покровов персонала. Их конструкторское исполнение предусматривает создание специальных защитных помещений на базе конференц-залов, столовых, кафе, которые продолжают повседневно использовать по прямому назначению посредством оснащения их стационарными фильтровентиляционными установками, обеспечивающими в них подпор воздуха при укрытии людей. Переносные коллективные средства защиты создаются на базе надувных палаток, сделанных из специальных изолирующих материалов, подпор воздуха в которых создается вмонтированной фильтровентиляционной установкой или вытравливанием сжатого воздуха (кислорода) из баллона через специальный редуктор.

Goncharenko Julia; Kachur Taras;
Miroshnik Oleg; Ryzhkin Alexei

Protection of objects of critical infrastructure from radioactive and chemical pollution of the atmosphere

The paper suggests a new conceptual approach to the problem of protecting personnel in critical infrastructure facilities. It is shown that radioactive particles as a result of the primary fission of nuclear material, radioactive particles resulting from secondary irradiation, radioactive gases and aerosols, as well as radionuclides formed upon activation of air nuclei, are the damaging factors of radioactive contamination of the atmosphere. Harmful factors of chemical pollution of the atmosphere are oxides, phenols, hydrocarbons, as well as aerosols of various chemical, including highly toxic substances, as well as decomposition and combustion products. They enter and are formed in the atmosphere as a result of nuclear explosions, technogenic accidents, fires of man-made and natural objects, as well as explosions of dirty radioactive and chemical bombs.

Most of the protective structures after the nineties were used for storage facilities and even for vegetable stores, as a result of which they came to a state that does not allow them to be used for the purpose for which they were intended. Some of them are in satisfactory and even good condition. However, the equipment is both physically and morally obsolete.

A new conceptual approach to protecting critical infrastructure facilities from radioactive and chemical pollution of the atmosphere is to create new collective protective equipment that is designed to protect the respiratory organs and skin of personnel. Their design execution provides for the creation of special protective premises on the basis of conference halls, canteens, cafes, which continue to be used on a daily basis for their intended purpose by equipping them with stationary filter-ventilation installations that provide air support in sheltering people. Portable collective protective equipment is created on the basis of inflatable tents made of special insulating materials, the air support in which is created by a built-in filter-ventilation installation or by etching compressed air (oxygen) from the balloon through a special reducer.

Відомості про авторів

Гончаренко Юлія Юріївна
Освіта: Повна вища (2010), магістр компьютерних наук.
Науковий ступінь: Доктор технічних наук (2015).
Вчене звання: Доцент.
Місце роботи: Державна установа «Інститут геохімії навколишнього середовища Національної академії наук України».
Область знань: Захіст інформації.
Наукові інтереси: Цивільний захист, захист критичної інфраструктури, захист інформації.

Качур Тарас Валентинович
Освіта: Повна вища (2016), магістр пожежної безпеки.
Місце роботи: Державна установа «Інститут геохімії навколишнього середовища Національної академії наук України».
Область знань:. Цивільний захист.
Наукові інтереси: Цивільний захист, захист критичної інфраструктури, фізичний захист.

Мирошник Олег Микалаевич
Освіта: Повна вища (2004), магістр пожежної безпеки.
Науковий ступінь: Кандидат технічних наук (2013).
Місце роботи: Державна установа «Інститут геохімії навколишнього середовища Національної академії наук України».
Область знань: Цивільний захист.
Наукові інтереси: Цивільний захист, захист критичної інфраструктури, фізичний захист.

Рижкін Олексій Сергійович
Освіта: Повна вища (2007), спеціаліст в галузі захисту інформації.
Місце роботи: Державна установа «Інститут геохімії навколишнього середовища Національної академії наук України».
Область знань: Захист інформації.
Наукові інтереси: Цивільний захист, захист критичної інфраструктури, фізичний захист.

УДК 551.463.2 + 004.386

ХАРАКТЕРИСТИКА ИНФОРМАЦИИ О СИТУАЦИОННОМ ФОНЕ ОКОЛО ОХРАНЯЕМОГО ОБЪЕКТА КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ (НА ПРИМЕРЕ АВТОМОБИЛЬНЫХ ТРАНСПОРТНЫХ СРЕДСТВ)

Азаренко Елена; Бородина Наталия; Касаткина Наталья; Камышенцев Геннадий; Лазаренко Сергей; Рыбка Евгений

Государственное учреждение «Институт геохимии окружающей среды НАН Украины»

CHARACTERISTICS OF THE SITUATIONAL BACKGROUND FOR A PROTECTED OBJECT OF CRITICAL INFRASTRUCTURE (ON THE EXAMPLE OF AUTOMOBILE VEHICLES)

Azarenko Elena; Borodina Natalia; Kasatkina Natalia; Kamyshentsev Genady; Lazarenko Sergei; Rybka Yevgeny

State Institution "Institute of Environmental Geochemistry of NASU"

Анотація: **Розглядаються основи нового концептуального підходу до виявлення ознак підготовки терористичних актів або інших ворожих дій проти охоронюваних об'єктів на прикладі використання ситуаційного фону автомобільних транспортних засобів близько охоронюваних об'єктів критичної інфраструктури.**

Ключові слова: **Охороняється об'єкт критичної інфраструктури, автомобільний транспортний засіб, ситуаційний фон, відеосистема, база даних і знань.**

Summary: **The basis of a new conceptual approach to identifying signs of preparation of terrorist acts or other hostile actions against protected objects is considered using the example of the use of the situational background of motor vehicles at protected critical infrastructure facilities.**

Key words: **Protected object of critical infrastructure, automobile vehicle, situational background, video system, database and knowledge.**

Введение

Термин «инфраструктура» произошел от двух латинских слов «infa» – «ниже, под», и «struktura» – «структура, расположение» [1]. Он означает комплекс взаимно связанных обслуживающих структур или объектов, составляющих и обеспечивающих основу функционирования системы.

В государственных предприятиях и учреждениях имеются специфические инфраструктуры, которые полноценно функционируют при наличии внешних, заграничных связей и обеспечивают инновационную [2], [3], рыночную [4], [5] и информационную [6] деятельность. Имеются и другие специфические инфраструктуры, например, военная [7], деятельность которых носит закрытый характер.

В связи с этим в каждом суверенном государстве выделяются сети, системы и сектора (совокупность элементов различных инфраструктур), от которых зависит жизнь граждан и существование общества, выход из строя или нарушение функционирования которых могло бы вызвать коллапс, паралич или хаос на общегосударственном, региональном или местном уровне. Комплекс таких секторов, систем или сетей называют критической инфраструктурой [8] – [11].

Работа каждого предприятия критической инфраструктуры направлена на решение определенной государственной задачи (производство топлива, получение электроэнергии, выпуск продукции и т. п.), которая требует привлечения человеческих ресурсов, транспортных средств, получения

материалов и других материальных, интеллектуальных, финансовых активов.

Движение материалов, людей, активов формирует определенный производственный поток или круговорот, который, в свою очередь, создает специфический производственный фон вокруг предприятия. Элементы этого фона в той или иной степени могут фиксироваться и отслеживаться системами наружного наблюдения [12], [13]. Регистрация изменений этого фона свидетельствует о нарушениях в функционировании предприятия, которые являются предпосылками к сбоям в работе, авариям, катастрофам и другим чрезвычайным ситуациям.

В соответствии с вышесказанным, разработка основ нового концептуального подхода к выявлению признаков подготовки террористического акта или других враждебных действий против охраняемых объектов на примере использования информации о ситуационном фоне автомобильных транспортных средств у охраняемых объектов критической инфраструктуры является актуальной и перспективной.

Основная часть

Характеристика охраняемых объектов критической инфраструктуры

В конце 90-х годов в связи с возрастанием террористической угрозы в развитых странах начались дискуссии об уязвимости национальных инфраструктур. Внимание экспертов было направлено не только на информационные (кибернетические) инфраструктуры, но и на все другие области обеспечения жизни общества.

В 1998 году директивой 63-го президента США была определена критическая инфраструктура как совокупность основных систем, которые имеют материальную или виртуальную платформу и воздействуют на фундаментальность экономики государства. К ним относят телекоммуникации, энергосистемы, банковский и финансовый секторы, транспортную систему, систему водообеспечения и спасательные службы. Затем почти все европейские государства стали заниматься критическими национальными инфраструктурами как совокупностью систем, нарушение функционирования хотя бы одной из которых может нанести серьезный ущерб экономике государства или привести к негативным социальным последствиями для общества.

В феврале 2003 года (уже после событий 11 сентября 2001 года) в США была принята Национальная стратегия физической охраны критической инфраструктуры. В ее состав, по сравнению с доктриной 1998 года, были включены ядерные электростанции, плотины, химическая промышленность, хранилища опасных веществ, базы оборонной промышленности. Сейчас по степени обеспечения безопасности объекты критической инфраструктуры принято разделять на три вида: 1) не охраняемые объекты, которые используют своих штатных сотрудников (охранников и сторожей) для обеспечения пропускного режима, контроля территории, сохранности материальных ценностей, для своевременного вызова подразделений патрульно-постовой службы полиции в случае нападения; 2) объекты, охраняемые вооруженной охраной, которую обеспечивают специальные охранные государственные или частные структуры; 3) объекты, имеющие специализированную службу физической защиты, предназначенную не только для охраны, но и защиты от вооруженного нападения.

В Украине длительное время велась дискуссия о том, что входит в критическую инфраструктуру, чем потенциально-опасный объект отличается от критически важного объекта. На законодательном уровне понятие о критической инфраструктуре в государстве не определено.

Указом Президентом № 8 от 16 января 2017 года введено в действие решение

Совета национальной безопасности и обороны «О совершенствовании мер обеспечения защиты объектов критической инфраструктуры». Данным Указом Кабинету Министров поручено в течение двух месяцев разработать и принять концепцию создания государственной системы защиты критической инфраструктуры, план мер по ее реализации и передать их на рассмотрение парламента. Службе безопасности Украины поручено принять меры по совершенствованию контрразведывательного обеспечения и защиты критической инфраструктуры.

Идентификационные признаки автомобильных транспортных средств, функционирующих около объектов критической инфраструктуры

Для обеспечения работы любого предприятия, тем более предприятий критической инфраструктуры, привлекаются различные транспортные средства, в первую очередь, автомобильные.

Кроме этого, в районе любого из вышеперечисленных охраняемых объектов критической инфраструктуры циркулирует большой поток автомобильных транспортных средств, которые осуществляют движение по различным маршрутам. К ним можно отнести транспорт, движущийся непосредственно на объект критической инфраструктуры и от него, доставляя различные грузы, сырье, запчасти и пр., обеспечивающий доставку сотрудников предприятия к рабочим местам и вывоз их с работы к местам проживания, а также доставку проверяющих (инспекторов) различных категорий, экскурсантов или корреспондентов и т. д. Другие транспортные средства аналогичным образом обеспечивают функционирование предприятий и учреждений, расположенных в непосредственной близости от охраняемого объекта. Третьи транспортные средства следуют транзитом через контролируемую зону охраняемого объекта.

Рассматривая теоретически вопрос антитеррористической безопасности объекта критической инфраструктуры все три множества транспортных средств, обеспечивающих охраняемый объект, обслуживающих соседние предприятия и учреждения и следующих транзитом, могут выступать в качестве потенциальных нарушителей (злоумышленников). Исходя из этого, первое разделение информации о транспортных средствах осуществляется по их принадлежности к охраняемому объекту: на объектовые, около объектовые и транзитные.

Чтобы выделить в этих множествах схожие подмножества, рассмотрим существующие характеристики автомобильных транспортных средств и выделим классификационные признаки, в соответствии с которыми в дальнейшем будем осуществлять идентификацию информации о транспортных средствах.

По назначению автомобильные транспортные средства делятся на грузовые, пассажирские и специальные. Первые предназначены для перевозки различных видов грузов. Ко вторым относятся транспортные средства, предназначенные для перевозки людей – автобусы и легковые автомобили. К специальным транспортным средствам относятся автомобили, предназначенные не только для транспортирования грузов или пассажиров, а и для монтажа специального оборудования и с целью выполнения соответствующих работ (автокраны, автовышки, подметальные, снегоуборочные, пожарные, автоподъемники и др.).

Конструктивные особенности каждого транспортного средства включают тип двигателя, колесную формулу, проходимость, наличие прицепа и другие детали.

Грузовые автомобили и автопоезда подразделяются по виду перевозок, определяющему тип кузова, на две группы: универсальные грузовики с кузовом

«бортовая платформа многоцелевого назначения» и специализированные грузовики, которые конструктивно приспособлены для перевозки одного или нескольких определенных видов грузов. В зависимости от дальности перевозок автомобили и автопоезда могут быть двух видов: для местных перевозок на расстояние в пределах 50 км; для дальних, междугородних перевозок.

Автобусы по конструкционной схеме подразделяются на три вида: одиночные, сочлененные, автобусные поезда, то есть автобус с прицепом. Одиночные автобусы применяются наиболее часто. Сочлененные автобусы применяются для улучшения маневренности автобусов большой вместимости. Автобусные поезда применяются ограниченно. Возможно применение прицепов для перевозки багажа, например, для обслуживания аэропортов. Имеются и двухэтажные автобусы.

По виду перевозок автобусы можно разделять на городские, пригородные, междугородные, местного сообщения, общего назначения, туристические, экскурсионные и школьные.

Легковые автомобили по конструкции кузова подразделяются на седаны, купе, универсалы, хечбеки. лимузины и другие, которые отличаются величиной рабочего объема двигателя, массой автомобиля и числом мест. При предельном между группами и классами рабочем объеме двигателя определяющим фактором считается сухая масса автомобиля. По виду перевозок легковые автомобили могут быть личные, служебные, такси и прокатные.

Следовательно, первая группа идентификационных признаков включает в себя десять подгрупп: 1) принадлежность к охраняемому объекту, который является собственником транспортного средства (объектовое, около объектовое, транзитное транспортное средство); 2) назначение (грузовое, пассажирское, специальное); 3) внешний вид (марка, цвет, повреждения и др.); 4) номер государственной, ведомственной или международной регистрации; 5) характеристики водителя транспортного средства; 6) тип и расположение двигателя; 7) конструктивные особенности транспортного средства; 8) наличие прицепа, буксира и других устройств; 9) наличие и характеристика пассажиров; 10) наличие и характеристика грузов.

По всем транспортным средствам, попадающим в зону контроля вокруг охраняемого объекта, составляется информационная база с идентификационными признаками, которые входят во вторую группу. Если первую группу идентификационных признаков условно можно назвать группой статических характеристик, так как они, в общем, постоянны и позволяют полностью идентифицировать автомобильное транспортное средство, то вторая группа – это группа динамических характеристик, которые описывают перемещение транспортных средств. То есть по каждому транспортному средству имеется набор динамических параметров, к которым можно применить такие качественные характеристики, как «обычно, постоянно, как всегда». Их будем называть штатными поведенческими или штатными. В них входят подгруппы характеристик, определяющих маршрут следования автомобиля: 1) пункт выезда; 2) пункт назначения; 3) время выезда; 4) время прибытия; 5) время и место остановок; 6) цель этих остановок и их продолжительность. Седьмая и последующие подгруппы характеристик даются в зависимости от конкретного вида транспортного средства. Рассмотрим это на следующих примерах транспорта из различных подгрупп.

Объектовые грузовые транспортные средства: № 1, предназначенные для вывоза мусора, № 2 – грузовик общего использования, № 3 – топливозаправщик (бензовоз).

Мусоровоз (транспортное средство № 1) в понедельник, среду и пятницу с 10 до 12 часов осуществляет сбор мусора, собранного в контейнеры, установленные в

специально оборудованных местах объекта. После сбора мусора, как правило, около 12 часов мусоровоз выезжает за пределы охраняемого объекта и следует на полигон бытовых отходов, расположенный в 35 км от объекта. Проезд до полигона и обратно с выгрузкой мусора занимает 1,5-2 часа, то есть в 13.30 – 14 часов мусоровоз возвращается обратно на объект. Так повторяется из недели в неделю, из месяца в месяц и является штатным вариантом использования транспортного средства № 1.

В отличие от мусоровоза топливозаправщик № 3 используется гораздо реже, как правило, 2-3 раза в месяц для доставки топлива в заправочную станцию гаража. Выезд осуществляется в будние дни в утренние часы, а возвращение – в обеденные.

Иначе обстоит дело с транспортным средством № 2, которое используется для доставки различных грузов, запчастей для оборудования и т. п. В течение года складывается картина, что ежемесячно транспортное средство № 2 выезжает 15-20 раз с утра до обеда, с обеда до вечера или с утра до вечера. Используется главным образом в будние дни, хотя может использоваться и в выходные, но это осуществляется по специальному разрешению руководителя объекта.

Около объектовые грузовые транспортные средства: № 11, предназначенные для перевоза хлебобулочных изделий (хлебовоз), № 22 – грузовик-рефрижератор для перевозки мяса, № 33 – грузовик с тентовым покрытием.

Хлебовоз каждое утро около 5 часов выезжает из города-спутника охраняемого объекта на хлебокомбинат, возвращается назад около 10 часов и в течение 2-3 часов развозит хлебную продукцию по магазинам, ларькам, учреждениям общественного питания. С 13 часов хлебовоз становится на стоянку и больше не используется.

Рефрижератор используется менее интенсивно, выезжает 2-3 раза в неделю из города-спутника вечером около 21 часа и возвращается с мясокомбината утром около 11 часов. Развозят продукцию по магазинам и учреждениям общественного питания в течение 2-4 часов. После 15 часов рефрижератор заезжает в гараж и в течение 2-3 суток не трогается.

Грузовик с тентовым покрытием за пределы города-спутника практически не выезжает, используется с 8-9 часов утра до 17-18 вечера для перевозки различных грузов со складов в магазины, из ларьков в гаражи и наоборот. Так повторяется еженедельно, из месяца в месяц и является штатным вариантом использования около объектовых транспортных средств № 11, № 22 и № 33.

Транзитные грузовые транспортные средства: № 111, предназначенное для перевозки автомобилей, № 222 – длиннобазовый фургон, предназначенный для перевозки различных грузов.

Автомобилевоз, как правило, 2 раза в месяц (с интервалом в 2 недели) проезжает в непосредственной близости от охраняемого объекта и следует из столицы в другие областные центры и только в одном направлении, назад возвращается другой дорогой, не проезжая мимо объекта.

Транспортное средство № 222 принадлежит транспортной компании и от 2 до 7 раз в месяц проезжает в одну сторону мимо объекта, а через 3-6 суток – в обратную. Подобные характеристики будут являться штатным вариантом использования транзитных транспортных средств № 111 и № 222.

Аналогично составляются штатные характеристики использования автобусов и легковых автомобилей. Систематизация данных о транспортных средствах, появляющихся в непосредственной близости от объекта, позволяет по каждому из них иметь набор штатных характеристик его использования. Это не только маршрут следования автомобиля, время и место парковки его на стоянке около объекта, время выезда с парковки и маршрут обратного следования, но и количество человек, приезжающих с водителем и уезжающих с ним, остановки с целью высадки (посадки) пассажиров, покупки

продуктов и заправки автомобиля и многое другое. Вся эта информация по дням недели, в выходные и праздничные дни, летом, осенью, зимой и весной позволяет формировать базы данных и знаний о всех транспортных средствах, функционирующих около объектов критической инфраструктуры. Совокупность полученных данных принято называть ситуационным фоном автомобильных транспортных средств, функционирующих около охраняемого объекта критической инфраструктуры.

В зависимости от пространственно-временных масштабов ситуационный фон разделяют на фрагменты, которые могут быть сезонными (весна, лето, осень, зима), внутрисезонными, недельными (будние дни, выходные и праздники), суточными (утро, день, вечер, ночь) и другими. На практике используется вся совокупность градаций для наименования одного фрагмента. Например, утренний воскресный летний фрагмент автомобильного транспортного фона.

Таким образом, базы данных и знаний о ситуационном фоне автомобильных транспортных средств, функционирующих у объектов критической инфраструктуры, формируются на основании групп идентификационных признаков. В них входят статические и динамические параметры, позволяющие однозначно определить автомобильное транспортное средство и штатный (стационарный, обычный, традиционный) характер его перемещения.

Отклонения от штатных характеристик использования транспортных средств

Каждый охраняемый объект критической инфраструктуры имеет системы оптоэлектронного наблюдения и оценки обстановки (видеосистемы). В общем случае они представляют собой системы телевизионного наблюдения замкнутого периметра, которые регулируют процесс визуального контроля с использованием оптико-электронных устройств, в том числе и инфракрасных, а также автоматического анализа изображений (распознавание лиц, номеров машин и т. д.). При этом они дают возможность вести наблюдение за автомобилями и людьми на любых расстояниях, просматривать архив событий, происходивших ранее. Видеосистемы наружного наблюдения также устанавливаются на предприятиях и учреждениях города-спутника объекта.

Кроме этого, объект и прилегающие к нему поселки и производственные площадки связаны автомобильными коммуникациями, на которых ключевые перекрестки, автомобильные мосты контролируются патрульно-постовой полицией. Для обеспечения безопасности автомобильного движения этим ведомством устанавливаются видеосистемы, которые обеспечивают контроль передвижения транспортных средств.

Передача всей регистрируемой видеосистемами информации, установленными в контролируемой зоне вокруг охраняемого объекта в реальном масштабе времени может быть реализована в установленном законодательством Украины порядке. Это позволяет иметь на охраняемом объекте постоянно обновляемую базу данных и знаний о ситуационном фоне автомобильных транспортных средств, функционирующих у объектов критической инфраструктуры. Чем больше информации о транспортном средстве будет накоплено, тем точнее будут характеристики его использования.

Программное обеспечение, используемое для анализа информации базы данных и знаний, позволяет при фиксации, для целей обеспечения безопасности охраняемого объекта транспортного средства выявлять отклонения от штатных характеристик его использования, которые разделяются по пяти уровням.

Для грузовых автомобилей отклонения от штатных характеристик использования (стационарности) 1-го уровня могут быть: остановка, нарушение Правил дорожного

движения, перевоз не заявленного груза, нарушение графика движения по объективным или субъективным причинам, нарушение графика или направления движения, существенное превышение скорости движения.

Для пассажирских транспортных средств (автобусов) отклонениями от стационарности 1-го уровня являются нарушения Правил дорожного движения, остановки в запрещенных местах, в том числе, не предусмотренных графиком движения, перевоз грузов вместо пассажиров, нарушение маршрута и расписания движения, существенное превышение скорости.

Для легковых автомобилей отклонениями от стационарности 1-го уровня являются выезд в нетипичное время, нарушение Правил дорожного движения, перевоз негабаритных грузов, перевоз пассажиров в количестве, большем, чем предусмотрено транспортным средством, остановка в запрещенных местах, существенное превышение скорости.

Отклонениями от стационарности 2-го уровня считается ситуация, когда одно и то же транспортное средство совершает 2-3 отклонения от штатных характеристик использования 1-го уровня в течение непродолжительного промежутка времени. Например, легковой автомобиль превысил скорость, затем остановился в месте, где остановка запрещена и т. д.

Также отклонением 2-го уровня считается событие, когда видеосистемой регистрируется автомобиль, информация о котором полностью отсутствует в базе данных. Безусловно, при длительном сборе данных в базу попадут сведения не только о сотрудниках объекта и работающих рядом с ним, а также о близких им людях: родственниках или друзьях, которые хотя бы раз в году заезжали в гости в город-спутник охраняемого объекта. Естественно, что часть данных о неизвестных автомобилях должна вводиться в базу данных и знаний операторами вручную. При этом оперативные работники или специалисты службы физической защиты в установленные сроки оповещают операторов. Тогда неизвестное транспортное средство становится известным.

Отклонениями от штатных характеристик использования транспортных средств 3-го уровня следует называть действия провокационного характера. Это происходит, когда известное транспортное средство в течение непродолжительного промежутка времени (до 15-20 минут) совершает 4-5 и более отклонений от штатных характеристик. Например, объектовый грузовик, следующий на объект, остановился в месте, где остановка запрещена, затем нарушает правило проезда железнодорожного переезда, превышает скорость, при обгоне задевает встречный автомобиль, но не останавливается и продолжает следовать дальше. Перед въездом на объект он (грузовик) начинает двигаться как обычно.

Также к 3-му уровню относятся действия явно провокационного характера. Например, когда гости (неизвестные), но на известном автомобиле, подъезжают не на стоянку, а к пункту пропуска персонала, останавливаются и, выйдя из машины, демонстративно распивают спиртные напитки, радуются по поводу праздника и выкрикивают нецензурные поздравления, оскорбления в адрес персонала или руководства и др.

К этому же уровню относятся действия, когда неизвестное транспортное средство с соблюдением всех Правил дорожного движения направляется непосредственно к объекту, даже если на нем установлены специальные сигнальные средства.

Отклонениями от стационарности 4-го уровня считаются опасные действия в отношении охраняемого объекта. Это происходит, когда известное транспортное средство, нарушая все штатные закономерности использования, известные для этого средства, нарушая Правила дорожного движения с явным превышением скорости движется в сторону объекта.

Другой вариант, когда несколько неизвестных транспортных средств с различных направлений движутся к охраняемому объекту. К этим ситуациям также относятся случаи, когда в двух и более количестве мест одновременно фиксируют известные или неизвестные транспортные средства, в которых пассажир угрожает водителю оружием или держит его направленным на водителя, пусть даже транспортное средство не движется в направлении охраняемого объекта.

Отклонениями от штатных характеристик использования транспортных средств 5-го уровня считаются враждебные действия или явно враждебные в отношении охраняемого объекта. Это происходит, когда известные или неизвестные транспортные средства с одной или нескольких сторон следуют к объекту с соблюдением правил или с превышением скоростного режима, при этом зафиксировано наличие оружия у водителей или пассажиров.

Отклонения от стационарности 3-5 уровней выводятся на главный пульт физической защиты объекта. Эти ситуации описаны в инструкциях и по ним службой физической охраны предпринимаются адекватные действия. Отклонения от штатных характеристик использования транспортных средств 1-го и 2-го уровня собираются в определенную группу в базе данных и знаний и анализируются специально подготовленным персоналом. На основании сделанных выводов происходит выявление признаков, характеризующих подготовку террористического акта или других враждебных действий в отношении охраняемого объекта.

Таким образом, регистрация, сбор, систематизация и последующий периодический анализ отклонений от штатных характеристик использования транспортных средств, функционирующих около охраняемых объектов критической инфраструктуры, позволяют заблаговременно выявлять признаки, характеризующие подготовку террористического акта или других враждебных действий в отношении охраняемого объекта.

Выводы

К охраняемым объектам критической инфраструктуры относятся атомные и гидроэлектростанции, химические и нефтехимические комбинаты, металлургические заводы и предприятия оборонной промышленности, телекоммуникационные центры (узлы связи) и множество других государственных предприятий и частных учреждений, выход из строя или нарушение функционирования которых может вызвать потерю управления или привести к существенным потерям на общегосударственном, региональном или местном уровне.

Базы данных и знаний о ситуационном фоне автомобильных транспортных средств, функционирующих у объектов критической инфраструктуры, формируются на основании групп идентификационных признаков. В них входят статические и динамические параметры, позволяющие однозначно определить автомобильное транспортное средство и штатный (стационарный, обычный, традиционный) характер его перемещения.

Регистрация, сбор, систематизация и последующий периодический анализ отклонений от штатных характеристик использования транспортных средств, функционирующих у охраняемых объектов критической инфраструктуры, позволяют заблаговременно выявлять признаки, характеризующие подготовку террористического акта, кибератаки или других враждебных действий в отношении охраняемого объекта.

Перелік посилань

[1] *Инфраструктура (Infrastructure) – это*. Доступ: http://forexaw.com/TERMs/Industry/Plants_and_soobruzheniya/l853.pdf

[2] В. П. Соловьев, *Инновационная инфраструктура как фактор социальной адаптации к условиям технологического развития.* Доступ: http://iee.org.ua/files/pub/svpinfr.pdf

[3] *Инновационная инфраструктура 2017-2021.* Кабинет министров Украины утвердил проект "Концепции Государственной целевой экономической программы развития инновационной инфраструктуры". Доступ: https://www.eduget.com/news/innovacionnaya_infrastruktura_2017-2021-357
[4] *Рыночная инфраструктура.* Доступ: http://econominfo.ru/view-article.php?id=31
[5] *Инфраструктура рынка. Формирование рыночной инфраструктуры в Украине.* Доступ: http://www.megos.org.ua/navczannia/ru/tema7.1.polit.page.html
[6] *Информационная инфраструктура.* Доступ: https://ru.wikipedia.org/wiki/%D0%98%D0
[7] *Военная инфраструктура это.* Доступ: *http://safety_buildings.academic.ru/71/%D0%92%D0*
[8] *Critical infrastructure – content, structure and problems of its protection.* Input: https://www.google.com.ua/?gfe_rd=cr&ei=gVWAWMT9FNKBYOfZnOAE&gws
[9] Л. Хофрейтер, *Критическая инфраструктура – содержание, структура и проблемы ее защиты.* Доступ: http:/jml2012.indexcopernicus.com/fulltxt.php?ICID=1129729
[10] *Указ Президента України №8/2017 від 16 січня 2017 року.* Доступ: http://www.president.gov.ua/documents/82017-21058
[11] *Порошенко усилил защиту объектов критической инфраструктуры.* Доступ: http://news.liga.net/news/politics/14672613poroshenko_usilil_zashchitu_obektov_kriticheskoy_infrastruktury.htm
[12] *Система телевидения замкнутого периметра.* Интернет публикация. 2010. - 5 с. Доступ: http//ru.wikipedia.org/wiki
[13] *Видеонаблюдение.* Интернет публикация. 2011. - 12 с. Доступ: http//www.3gkiev.com

References

[1] *Infrastructure is.* Access: http://forexaw.com/TERMs/Industry/Plants_and_soobruzheniya/l853.pdf
[2] V. P. Soloviev, *Innovative infrastructure as a factor of social adaptation to the conditions of technological development.* Access: http://iee.org.ua/files/pub/svpinfr.pdf
[3] *Innovative Infrastructure 2017-2021.* The Cabinet of Ministers of Ukraine approved the draft "Concept of the State Targeted Economic Program for the Development of Innovation Infrastructure." Access: https://www.eduget.com/news/innovacionnaya_infrastruktura_2017-2021-357
[4] *Market infrastructure.* Access: http://econominfo.ru/view-article.php?id=31
[5] *Market Infrastructure. Formation of market infrastructure in Ukraine.* Access: http://www.megos.org.ua/navczannia/en/tema7.1.polit.page.html
[6] *Information infrastructure.* Access: https://en.wikipedia.org/wiki/%D0%98%D0
[7] *Military infrastructure is.* Access: http://safety_buildings.academic.com/71/%D0%92%D0
[8] *Critical infrastructure - content, structure and problems of its protection.* Input: https://www.google.com.ua/?gfe_rd=cr&ei=gVWAWMT9FNKBYOfZnOAE&gws
[9] L. Hofreiter, *Critical infrastructure - the content, structure and problems of its protection.* Access: http: /jml2012.indexcopernicus.com/fulltxt.php?ICID = 1129729
[10] *Decree of the President of Ukraine No. 8/2017 dated 16 December 2017.* Access: http://www.president.gov.ua/documents/82017-21058
[11] *Poroshenko strengthened the protection of critical infrastructure facilities.* Access: http://news.liga.net/news/politics/14672613-poroshenko_usilil_zashchitu_obektov_kritiches koy_infrastruktury.htm
[12] *The closed-circuit television system.* Internet publication. 2010. - 5 p. Access: http // en.wikipedia.org / wiki
[13] *Video surveillance.* Internet publication. 2011. - 12 with. Access: http // www.3gkiev.com

Реферат

Азаренко Олена; Бородіна Наталія; Касаткіна Наталія; Камишенцев Генадій; Лазаренко Сергій; Рибка Євген

Характеристика інформації ситуаційного фону біля об'єкта критичної інфраструктури, що охороняється (на прикладі автомобільних транспортних засобів)

Робота присвячена розробці основ нового концептуального підходу до виявлення ознак підготовки терористичного акту або інших ворожих дій проти об'єктів, що охороняються, на прикладі використання ситуаційного фону автомобільних транспортних засобів біля об'єктів критичної інфраструктури.

У роботі спочатку дана характеристика об'єктів критичної інфраструктури, що охороняються. Показано, що до об'єктів критичної інфраструктури відносяться атомні і гідроелектростанції, хімічні і

нафтохімічні комбінати, металургійні заводи і підприємства оборонної промисловості, телекомунікаційні центри (вузли зв'язку) і безліч інших державних підприємств і приватних установ, вихід з ладу або порушення функціонування яких може викликати втрату управління або привести до істотних втрат на загальнодержавному, регіональному або місцевому рівні. Розглянуто ідентифікаційні ознаки автомобільних транспортних засобів, що функціонують у об'єктів критичної інфраструктури. Виділено дві групи ознак, відповідно до яких проводиться збір даних. Перша група ідентифікаційних ознак включає в себе десять підгруп: 1) приналежність до об'єкту охорони (об'єктовий, близько об'єктовий, транзитний транспортний засіб); 2) призначення (вантажний, пасажирський, спеціальний); 3) зовнішній вигляд (марка, колір, пошкодження щодо); 4) номер державної, відомчої або міжнародної реєстрації; 5) характеристики водія транспортного засобу; 6) тип і розташування двигуна; 7) конструктивні особливості транспортного засобу; 8) наявність причепа, буксира та інших пристроїв; 9) наявність і характеристика пасажирів; 10) наявність і характеристика вантажів. Цю групу ідентифікаційних ознак називають групою статичних характеристик, так як вони повністю дозволяють ідентифікувати автомобільний транспортний засіб.

Друга група – це динамічні характеристики, які описують переміщення транспортних засобів. У неї входять підгрупи характеристик, що визначають маршрут прямування автомобіля: 1) пункт виїзду; 2) пункт призначення; 3) час виїзду; 4) час прибуття; 5) час і місце зупинок; 6) мета цих зупинок та їх тривалість. Сьома і наступні підгрупи характеристик даються в залежності від конкретного виду транспортного засобу.

Систематизація даних, про транспортні засоби, що з'являються в безпосередній близькості з об'єктом, дозволяє по кожному транспортному засобу мати набір штатних характеристик його використання. Це не тільки маршрут прямування автомобіля, час і місце парковки його на стоянці біля об'єкта, час виїзду з парковки і маршрут зворотного прямування. Це і кількість осіб, які приїжджають з водієм і виїжджаючих з ним, це і зупинки з метою висадки (посадки) пасажирів, покупки продуктів і заправки автомобіля, і багато іншого. Вся ця інформація по днях тижня, у вихідні та святкові дні, влітку, восени, взимку і навесні дозволяє формувати бази даних і знань про всі транспортні засоби, що функціонують у об'єктів критичної інфраструктури. Сукупність цих даних прийнято називати ситуаційним фоном автомобільних транспортних засобів, що функціонують біля об'єкту критичної інфраструктури, що охороняється.

Чим більше фіксацій транспортного засобу буде виконано, тим точніше будуть отримані штатні характеристики його використання. Показано, що реєстрація, збір, систематизація і наступний періодичний аналіз відхилень від штатних показників використання транспортних засобів, що функціонують біля об'єктів критичної інфраструктури, що охороняються, дозволяє завчасно виявляти ознаки, які характеризують підготовку терористичного акту або інших ворожих дій щодо об'єкту, що охороняється.

Азаренко Елена; Бородина Наталья; Касаткина Наталья; Камышенцев Геннадий; Лазаренко Сергей; Рыбка Евгений

Характеристика информации о ситуационном фоне около охраняемого объекта критической инфраструктуры (на примере автомобильных транспортных средств)

Работа посвящена разработке основ нового концептуального подхода к выявлению признаков подготовки террористического акта или других враждебных действий против охраняемых объектов на примере

использования ситуационного фона автомобильных транспортных средств около охраняемых объектов критической инфраструктуры.

В работе первоначально дана характеристика охраняемых объектов критической инфраструктуры. Показано, что к ним относятся атомные и гидроэлектростанции, химические и нефтехимические комбинаты, металлургические заводы и предприятия оборонной промышленности, телекоммуникационные центры (узлы связи) и множество других государственных предприятий и частных учреждений, выход из строя или нарушение функционирования которых может вызвать потерю управления или привести к существенным потерям на общегосударственном, региональном или местном уровне.

Рассмотрены идентификационные признаки автомобильных транспортных средств, функционирующих у объектов критической инфраструктуры. Выделены две группы признаков, в соответствии с которыми производится сбор данных. Первая группа идентификационных признаков включат в себя десять подгрупп: 1) принадлежность к охраняемому объекту, который является собственником транспортного средства (объектовое, около объектовое, транзитное транспортное средство); 2) назначение (грузовое, пассажирское, специальное); 3) внешний вид (марка, цвет, повреждения и др.); 4) номер государственной, ведомственной или международной регистрации; 5) характеристики водителя транспортного средства; 6) тип и расположение двигателя; 7) конструктивные особенности транспортного средства; 8) наличие прицепа, буксира и других устройств; 9) наличие и характеристика пассажиров; 10) наличие и характеристика грузов. Эту группу идентификационных признаков называют группой статических характеристик, так как они полностью позволяют идентифицировать автомобильное транспортное средство.

Вторая группа – это группа динамических характеристик, которые описывают перемещение транспортных средств. В нее входят подгруппы характеристик, определяющих маршрут следования автомобиля: 1) пункт выезда; 2) пункт назначения; 3) время выезда; 4) время прибытия; 5) время и место остановок; 6) цель этих остановок и их продолжительность. Седьмая и последующие подгруппы характеристик даются в зависимости от конкретного вида транспортного средства.

Систематизации данных, о транспортных средствах, появляющихся в непосредственной близости с объектом, позволяет по каждому транспортному средству иметь набор штатных характеристик его использования. Это не только маршрут следования автомобиля, время и место парковки его на стоянке около объекта, время выезда с парковки и маршрут обратного следования. Это и количество человек, приезжающих с водителем и уезжающих с ним, это и остановки с целью высадки (посадки) пассажиров, покупки продуктов и заправки автомобиля, и многое другое. Вся собранная информация по дням недели, в выходные и праздничные дни, летом, осенью, зимой и весной позволяет формировать базы данных и знаний о всех транспортных средствах, функционирующих у объектов критической инфраструктуры. Совокупность полученных данных принято называть ситуационным фоном автомобильных транспортных средств, функционирующих около охраняемого объекта критической инфраструктуры. Чем больше фиксаций транспортного средства будет выполнено, тем точнее

получатся штатные характеристики его использования.

Показано, что регистрация, сбор, систематизация и последующий периодический анализ отклонений от штатных характеристик использования транспортных средств, функционирующих около охраняемых объектов критической инфраструктуры, позволяют заблаговременно выявлять признаки, характеризующих подготовку террористического акта или других враждебных действий в отношении охраняемого объекта.

Azarenko Elena; Borodina Natalia; Kasatkina Natalia; Kamyshentsev Genady; Lazarenko Sergei; Yevgeny Rybka

Characteristics of the situational background for a protected object of critical infrastructure (on the example of automobile vehicles)

The work is devoted to the development of the foundations of a new conceptual approach to identifying signs of preparing a terrorist act or other hostile actions against protected objects using the example of the use of the situational background of motor vehicles in protected critical infrastructure facilities.

The work initially gave a description of the protected objects of critical infrastructure. It has been shown that nuclear and hydroelectric power plants, chemical and petrochemical plants, metallurgical plants and enterprises of the defense industry, telecommunication centers (communication centers) and a lot of other state enterprises and private institutions are among the critical infrastructure objects that are protected, the failure or malfunction of which can cause a loss Management or lead to significant losses at the national, regional or local level. Identification features of motor vehicles operating near critical infrastructure facilities are considered. Two groups of characteristics are identified according to which data are collected. The first group of identification signs includes ten subgroups. The first - belonging to the protected object (object, near the object, transit vehicle) and the owner of the vehicle. The second is the destination (cargo, passenger, special). Third - Appearance (brand, color, damage, etc.). The fourth is the number of state, departmental or international registration. The fifth is the characteristics of the driver of the vehicle. The sixth is the type and location of the engine. Seventh - Design features of the vehicle. Eighth - the presence of a trailer, tug and other devices. The ninth - the availability and characteristics of passengers. Tenth - the availability and characteristics of goods. This group of identification features is called a group of static characteristics, since they completely allow the identification of an automobile vehicle. The second group is a group of dynamic characteristics that describe the movement of vehicles. It includes subgroups of characteristics that determine the route of the car. The first is the point of departure. The second is the destination. The third is the time of departure. The fourth is the time of arrival. The fifth is the time and place of the stops. The sixth is the purpose of these stops and their duration. Seventh and subsequent subgroups of characteristics are given depending on the type of vehicle. Systematization of data, about vehicles appearing in close proximity to the object, allows for each vehicle to have a set of standard characteristics of its use. This is not only the route of the car, the time and place of parking it in the parking lot near the facility, the time of departure from the parking lot and the route of the return journey. This and the number of people coming with the driver and leaving with him, it's stopping for the purpose of landing

(landing) of passengers, buying food and refueling the car, and much more. All this information on the days of the week, on weekends and holidays, in summer, autumn, winter and spring allows you to create databases and knowledge of all vehicles operating near critical infrastructure facilities. The totality of these data is usually called the situational background of motor vehicles operating near the protected critical infrastructure facility.

The more fixations of the vehicle will be performed, the more accurate will be the staff characteristics of its use. It is shown that the registration, collection, systematization and subsequent periodic analysis of deviations from the standard characteristics of the use of vehicles operating in the protected facilities of critical infrastructure, allows early detection of signs characterizing the preparation of a terrorist act or other hostile actions with respect to a protected facility.

Відомості про авторів

Азаренко Олена Василівна

Освіта: Повна вища (1987), математик, викладач.

Науковий ступінь: Доктор фізико-математичних наук (2007).

Вчене звання: Професор.

Місце роботи: Державна установа «Інститут геохімії навколишнього середовища Національної академії наук України».

Область знань: Інформаційні технології.

Наукові інтереси: Цивільний захист, захист критичної інфраструктури, фізичний захист.

Бородина Наталія Анатоліївна

Освіта: Повна вища (2001), магістр екології.

Науковий ступінь: Кандидат технічних наук (2007).

Вчене звання: Старший науковий співробітник.

Місце роботи: Державна установа «Інститут геохімії навколишнього середовища Національної академії наук України».

Область знань: Інформаційні технології.

Наукові інтереси: Цивільний захист, захист критичної інфраструктури, фізичний захист.

Касаткіна Наталія Вікторівна

Освіта: Повна вища (1983), інженер-механік.

Науковий ступінь: Кандидат технічних наук (2009).

Місце роботи: Державна установа «Інститут геохімії навколишнього середовища Національної академії наук України».

Область знань:. Інформаційні технології.

Наукові інтереси: Цивільний захист, захист критичної інфраструктури, фізичний захист.

Камишенцев Генадій Володимирович

Освіта: Повна вища (2014), спеціаліст в галузі захисту інформації.

Місце роботи: Державна установа «Інститут геохімії навколишнього середовища Національної академії наук України».

Область знань: Захист інформації.

Наукові інтереси: Цивільний захист, захист критичної інфраструктури, фізичний захист.

Лазаренко Сергій Володимирович

Освіта: Повна вища (1987).

Науковий ступінь: Кандидат технічних наук (2007).

Вчене звання: Доцент.

Місце роботи: Державна установа «Інститут геохімії навколишнього середовища Національної академії наук України».

Область знань: Захист інформації.

Наукові інтереси: Цивільний захист, захист критичної інфраструктури, фізичний захист.

Рибка Євген Алексиевич

Освіта: Повна вища (2008), магістр пожежної безпеки.

Науковий ступінь: Кандидат технічних наук (2013).

Місце роботи: Державна установа «Інститут геохімії навколишнього середовища Національної академії наук України».

Область знань: Інформаційні технології.

Наукові інтереси: Цивільний захист, захист критичної інфраструктури, фізичний захист.

УДК 004.49

СТРУКТУРНІ ЗАКОНОМІРНОСТІ ЕВОЛЮЦІОНУВАННЯ МЕТАМОРФНОГО ШКІДЛИВОГО ПЗ

Кожокар Владислав; Стьопочкіна Ірина
КПІ ім. Ігоря Сікорського

STRUCTURAL PATTERNS IN METAMORPHIC MALWARE EVOLUTION

Kozhokar Vladyslav; Stopochkina Iryna
Igor Sikorsky Kyiv Polytechnic Institute

Анотація: **Запропоновано характеристики, які можуть використовуватись для виявлення, класифікації та кластеризації шкідливого ПЗ метаморфного типу. Виявлено характер залежностей між оригіналом та метаморфними нащадками.**
Ключові слова: **Метаморфне шкідливе програмне забезпечення, антивірусний захист, кластеризація, класифікація шкідливого ПЗ, статичний аналіз**.
Summary: **The characteristics for metamorphic malware detection, classification and clasterization are proposed**. **The nature od structural dependencies between original and metamorphic descendants is shown.**
Keywords: **Metamorphic malware, virus protection, malware clustering and classifying, static analysis**.

Вступ

Антивірусні компанії помічають зростання випадків появи шкідливого програмного забезпечення, яке має функції самомодифікації. Таким є ПЗ із властивостями метаморфування. Виявлення цих видів шкідливого ПЗ за допомогою антивірусних продуктів, які працюють, засновуючись на традиційному сигнатурному підході, є неефективним, оскільки структурна форма такого ПЗ постійно змінюється і відповідним чином змінюються й сигнатури. При цьому функціональність зміненої копії ПЗ залишається тією ж самою. Застосування засобів поведінкового аналізу не завжди дають бажані результати, оскільки шкідливе ПЗ "розпізнає" віртуалізацію і змінює свою поведінку, приховуючи на час дослідження шкідливий функціонал.

В роботі [1] показано можливість використання опкодів для встановлення факту шкідливості ПЗ (без відношення до певного класу), а в роботі [2] було застосовано статистичний аналіз опкодів до задачі класифікації метаморфного шкідливого ПЗ. Однак характер залежностей між оригіналом та нащадками продемонстрований не був. Тому доцільно розглянути інші засоби виявлення структурної подібності між зразками.

Актуальною задачею є дослідження метаморфних зразків на основі різних підходів (в тому числі не характерних для аналізу бінарних файлів) та встановлення закономірностей еволюціонування метаморфного зразка. За звітами антивірусних компаній є роботи [3], які ілюструють принцип дії метаморфного шкідливого ПЗ й дозволяють зробити припущення про закономірності метаморфних змін та використати це при дослідженні структурних особливостей споріднених метаморфних зразків.

Постановка задачі

Метою даної роботи є визначення характеристик, які можуть слугувати індикаторами схожості для ПЗ метаморфного типу. Ці характеристики можуть бути вихідним матеріалом для алгоритмів класифікації й кластеризації. Також у роботі наведені результати експериментальних досліджень структурної подібності між оригіналом та нащадками.

Структура та принципи еволюції метаморфного зразка

Згідно звітів антивірусних компаній можна виділити основні принципи функціонування механізму еволюції метаморфного шкідливого зразка.

Основні техніки, які використовуються метаморфними вірусами, полягають у перетворенні вихідного тексту або виконуваного коду програми таким чином, щоб зберігати свою функціональність і в результаті ускладнювати процес аналізу при декомпіляції Фактично це типові прийоми обфускації. Їх слід на поділити на наступні види:

1) перейменування методів, класів та інших змінних для масимального ускладнення при дизасемблюванні;

2) заміна одних конструкцій мови асемблер іншими, з іншим бінарним представленням, однак із тим самим функціоналом;

3) заміна статичних членів на виклики методів;

4) введення додаткових блоків, які не змінюють функціонал програми, до структури програми;

5) зміна розташування даних з використанням об’єднання та роз’єднання даних;

6) перестановки вершин графу виконання програми, які не змінюють функціонал.

Зазвичай метаморфний модуль, який здійснює перетворення основного коду шкідливого ПЗ, має містити такі основні компоненти:

1) дизасемблер;
2) оптимізатор/стискувач опкодів (shrinker);
3) розширювач опкодів (expander);
4) перестановщик (swapper);
5) переміщувач (relocator);
6) засмічувач (garbager);
7) прибиральник.

Внутрішній дизассемблер виконує зворотні перетворення коду.

“Shrinker” стискає, оптимізує дві та більше інструкцій в одну.

Розширювач, навпаки, розширює одну інструкцію до більш ніж однієї.

Перестановщик міняє місцями дві чи більше команд.

“Relocator” перераховує всі відносні посилання (стрибки, виклики і покажчики).

“Garbager” встановлює одну чи більше порожніх інструкції між реальним кодом. Це можуть бути порожні інструкції nop, або комбінації інструкцій.

Прибиральник навпаки прибирає засмічуючий код, вставлений засмічувачем.

Еволюція метаморфного вірусу здійснюється у наступній послідовності:

1. Вірусний код дизасемблюється в проміжну форму, яка не залежить від апаратної платформи (процесора), на якій виконується код. Це робить можливим створення коду для різних операційних систем або навіть різних процесорів.

2. Проміжна форма скорочується шляхом видалення зайвих та невикористовуваних інструкцій. Ці інструкції були додані в попередніх реплікаціях, щоб заважати дизасемблюванню сторонніми особами.

3. Виконуються перестановки підпрограм чи блоків коду, пов'язуючи їх з інструкціями переходу.

4. Код знов розширюється шляхом додавання надлишкових і невикористовуваних інструкцій.

5. З проміжної компонується кінцева форма, яка буде додана до заражених файлів.

Щоб здійснювати мутацію код з покоління в покоління, метаморфним вірусам потрібно вміти аналізувати свій власний код. Це означає, що складність перетворень в попередніх поколіннях чинить безпосередній вплив на те, як вірус аналізує і перетворює код. Отже, для забезпечення достатньої швидкодії метаморфні перетворення мають бути не занадто складними, і зворотніми. Кількість перетворень (зокрема, підстановок та перестановок коду) є скінченою. При необхідності зберігати незмінність функціоналу шкідливого ПЗ ця кількість значно обмежується. Отже, слід припустити, що при еволюції можуть з’являтись як достатньо відмінні від оригіналу нащадки, так і дуже схожі. Теоретично можуть з’являтись нащадки, що є копією оригінала.

За таких умов структура зразків одного сімейства має зберігати значну міру схожості.

Характер змін за опкодами

Приведемо результати експерименту з метаморфними зразками, які дозволяє виявити характер змін за опкодами між оригіналом та нащадками.

В табл. 1 показано, як змінюється кількість найбільш значущих опкодів в модифікаціях оригінала віруса Hunatcha. Модифікації одержані за допомогою метаморфного модуля metame, а зразки вірусів взяті з ресурсу vxheaven.org.

Модифікації одержано до 10-го нащадка. Але для скорочення викладення результатів експерименту наведемо лише дані щодо перших трьох нащадків (мод.1, мод.2, мод.3). Як бачимо, змінюються не всі опкоди, а лише деякі (виділено жирним шрифтом).

Таблиця 1.

Зміни кількості опкодів в модифікаціях Hunatcha

Hunatcha	**Ориг.**	**Мод.1**	**Мод.2**	**Мод.3**
ADD	115	115	115	115
AND	6	6	6	6
CALL	191	191	191	191
CMP	103	103	103	103
J(COND)	197	197	197	197
JMP	111	111	111	111
LEA	185	185	185	185
LEAVE	0	0	0	0
MOV	**727**	**724**	**721**	**722**
NEG	1	1	1	1
NOP	**18**	**21**	**22**	**23**
NOT	9	9	9	9
OR	**5**	**6**	**9**	**8**
POP	**112**	**115**	**119**	**117**
PUSH	**80**	**83**	**87**	**85**
RET	63	63	63	63
SHL	4	4	4	4
SHR	1	1	1	1
SUB	**62**	**64**	**63**	**64**
TEST	**92**	**91**	**88**	**89**
XCHG	2	2	2	2
XOR	**66**	**64**	**65**	**64**

Для порівняння наведено дані щодо модифікацій спорідненого віруса HunatchaB.

Таблиця 2.

Зміни кількості опкодів в модифікаціях HunatchaB

HunatchaB	**Ориг.**	**Мод.1**	**Мод.2**	**Мод.3**
ADD	115	115	115	115
AND	6	6	6	6
CALL	203	203	203	203
CMP	103	103	103	103
J(COND)	197	197	197	197
JMP	**137**	**111**	**111**	**111**
LEA	209	209	209	209
LEAVE	0	0	0	0
MOV	**771**	**766**	**767**	**769**
NEG	1	1	1	1
NOP	19	22	21	19
NOT	9	9	9	9
OR	**5**	**6**	**7**	**7**
POP	**112**	**118**	**117**	**115**
PUSH	**80**	**86**	**85**	**83**
RET	64	64	64	64
SHL	4	4	4	4
SHR	1	1	1	1
SUB	**62**	**63**	**63**	**63**
TEST	**92**	**91**	**90**	**90**
XCHG	2	2	2	2
XOR	**66**	**65**	**65**	**65**

Як слідує з табл. 2, збільшення кількості команд нащадків відносно оригіналу відбулося для *mov*, *nop*, *or*, *pop*, *push* та *sub*, а відповідно зменшення відбулося у *jmp*, *mov*, *test* та *xor*.

Обчислимо відстань Мінковського за оригіналом віруса Hunatchab та нащадками деяких інших вірусів (табл. 3) за формулою:

$$d = \left(\sum_{i=1}^{n} \left|x_i - y_i\right|^{\rho}\right)^{1/\rho}, \qquad (1)$$

де x_i та y_i – кількість опкодів i-того виду в оригіналі та нащадку відповідно. Візьмемо p=2 (Евклідова відстань).

ISSN 2074-9481

Таблиця 3.

Відстань Мінковського

Hunatchab	**Мод.1**	**Мод.2**	**Мод.3**
BatzBack	0,30659	0,30648	0,30627
Branko	0,07333	0,07302	0,07248
BullMoose	0,16540	0,16585	0,16681
Clibo	0,11347	0,11370	0,11422
Hunatcha	0,02155	0,02182	0,02242
Hunatchab	**0,01250**	**0,01227**	**0,01190**

З табл. 3 слідує, що показник *d* є найближчим до нуля при порівнянні із спорідненим оригіналом. Для віруса Hunatcha його модифікації виявились теж досить близькими, оскільки цей вірус є спорідненим. З іншого боку, значення одержані для модифікацій Branko, можуть ввести дослідника в оману щодо спорідненості цих зразків.

Графічне представлення шкідливих зразків та аналіз за індексом структурної відповідності

Представимо бінарний файл шкідливого зразка у вигляді чорно-білого зображення на рис. 1 щоб встановити, наскільки цим видам шкідливого ПЗ притаманне збереження певних рис структури. Спостерігається певне чередування однорідних зон, що може вказувати на прояв структури. Про те, як будуть відрізнятись графічні представлення шкідливого ПЗ, яке належить до одного сімейства, свідчить навіть без проведення спеціального аналізу зображення на рис. 2 та рис. 3. Вони мають певні схожі риси, хоча вони істотно відрізняються від представника іншого сімейства, представленого на рис. 1.

Для більш детального аналізу шкідливих зразків використаємо показники SSIM (співвідношення (2)), які традиційно використовуються для аналізу подібності графічних зображень [4].

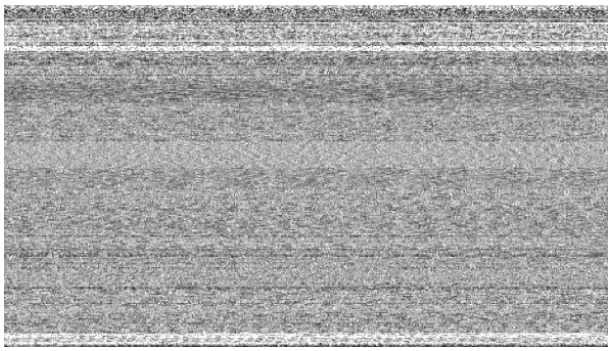


Рис. 1 – Графічне представлення вірусу BatzBack

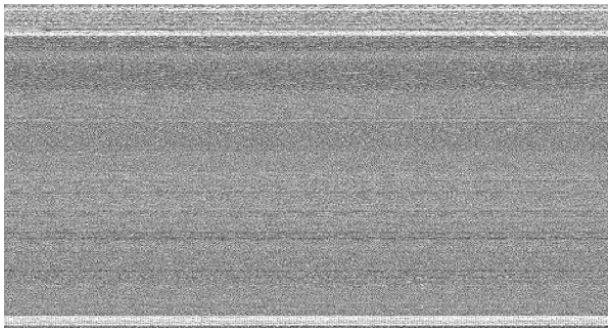


Рис. 2 – Графічне представлення вірусу Hunatcha

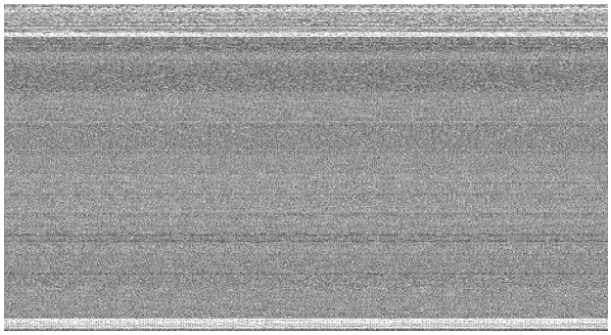


Рис. 3 – Графічне представлення вірусу HunatchaB

$$SSIM\left(x,y\right)=\frac{(2\mu_x\mu_y+c_1)(2\sigma_{xy}+c_2)}{(\mu_x^2+\mu_y^2+c_1)(\sigma_x^2+\sigma_y^2+c_2)}, \quad (2)$$

де μ_x – математичне очікування (МО) послідовності бітів 1-го зразка;

μ_y – МО послідовності бітів 2-го зразка;

σ_x – дисперсія послідовності бітів 1-го зразка;

σ_y – дисперсія послідовності бітів 2-го зразка;

σ_{xy} – коваріація послідовності бітів 1-го та 2-го зразка;

$c_1=(k_1L)^2$, $c_2=(k_2L)^2$ — стабілізуючі змінні, L — динамічний діапазон пікселів (зазвичай $2^{(\text{bits per pixel})}$-1). По замовчуванню приймаємо $k_1=0{,}01$, $k_2=0{,}03$.

За обчисленими значеннями індексів структурної відповідності SSIM відносно оригіналу вірусу Hunatcha та модифікацій інших вірусів (табл. 4) слідує, що спорідненість прослідковується достатньо чітко. Близькі до нуля значення свідчать про відсутність структурної схожості, тоді як близькі до одиниці значення свідчать про структурну ідентичність чи подібність.

Таблиця 4.

Значення індекса SSIM

Hunatcha	**Мод.1**	**Мод.2**	**Мод.3**
BatzBack	0,29263	0,29178	0,29158
Branko	0,02242	0,02283	0,02242
BullMoose	0,21823	0,21901	0,21889
Clibo	0,02218	0,02247	0,02100
Hunatcha	0,92370	0,93567	0,84787
Hunatchab	0,36476	0,36492	0,36496

В табл. 4 показано типову ситуацію, коли значення індексу SSIM 0,8 та вище свідчать про спорідненість зразків, тоді як значення, які є меншими 0,5 свідчать про неспорідненість (чи слабку схожість) зразків.

Застосування функцій нечіткого хешування

При встановленні схожості деяких типів файлів, в тому числі й виконуваних, ефективно застосовуються функції нечіткого хешування [5]. Зауважимо, що функції нечіткого хешування спеціалізовані на виявленні подібностей у текстах, та базуються на показниках типу “зважена редакторська відстань” (weighted edit distance).

Спробуємо використовувати їх для аналізу схожості метаморфних зразків. При використанні функції ssdeep в серії експериментів було встановлено, що міра схожості представників одного сімейства становить від 50 до 97 при шкалі оцінювання від 0 до 100 (0- схожості не встановлено, 100 – зразки ідентичні). Чим меншим є розмір шкідливого зразка, тим спостерігався вищий показник схожості з оригіналом. Це зумовлено тим, що на невеликих шкідливих зразках складно застосувати значну кількість перетворень, не змінивши функціонал. Наприклад, зразок Hunatcha, написаний на мові C, складається із трохи більше 100 рядків вихідного коду.

Найвища ступінь несхожості спостерігається між оригіналом та першим нащадком. При наступній еволюції зразки змінюються вже не так сильно. Однак, спорідненість ланцюжка нащадків та оригіналу можна встановити.

Кластеризація й класифікація метаморфних зразків

Визначимо послідовність дій, які можна застосувати при вирішенні задач кластеризації та класифікації метаморфних зразків.

Наведемо цю послідовність у вигляді схеми на рис. 4.

Результати дослідження (за наявності нечіткої трактовки) можуть бути подані на вхід алгоритмів кластеризації та класифікації для виявлення прихованих закономірностей.

З схеми на рис. 4 слідує, що можна виділити три основні напрямки: 1) аналіз за опкодами (це можуть бути N-грами опкодів чи аналіз за кількістю найважливіших опкодів, як було розглянуто нами раніше) – цей спосіб потребує попереднього дизасемблювання зразка, та схильний давати хибно-позитивні результати, однак, він може застосовуватись для того, щоб не враховувати зразки, які є очевидно неспорідненими; 2) аналіз за індексом SSIM - спосіб здатний вловлювати структурну спорідненість, а не лише числові відповідності в опкоді, як спосіб 1); 3) одержання дампу вихідного зразка та його аналіз за допомогою утиліти нечіткого хешування – цей спосіб є менш чутливим за способи 1), 2) до наявності спорідненостей, однак, дозволяє звернути увагу на ті результати, які потенційно можуть бути хибнопозитивними.

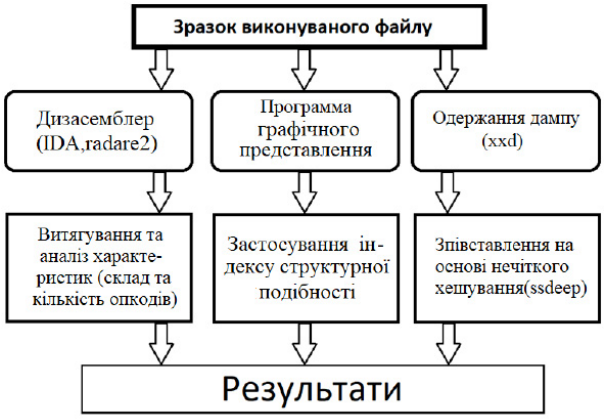


Рис. 4 – Схема послідовності дослідження метаморфного зразка

Способи 1) – 3), розглянуті в даній роботі, мають застосовуватись в комплексі при аналізі спорідненості метаморфних зразків.

Висновки

Проведені експерименти підтвердили , що метаморфні перетворення, які забезпечують еволюцію оригінального зразка, не знищують у повній мірі структурну подібність між оригіналом та нащадками. Цю структурну подібність цілком можливо встановити за допомогою таких способів: 1) аналіз за опкодами (відстань Мінковського за кількістю опкодів *i*-го виду), 2) аналіз за показниками структурної подібності SSIM, 3) аналіз за допомогою нечітких функцій хешування.

В перспективі для антивірусного захисту для виявлення факту шкідливості зразка ПЗ слід застосовувати ще й інші методи, які не розглядались в даній роботі. Однак, при вирішенні задач кластеризації та класифікації метаморфних шкідливих зразків доцільно використовувати комбінацію наведених трьох способів виділення характеристик, які дозволять більш ефективно використовують алгоритми, на вхід яких вони будуть подані. Як слідує із прикладів, наведених у статті, інколи за вказаними характеристиками (у випадку вірусів невеликого розміру) можна встановити факт спорідненості зразків без використання додаткових алгоритмів класифікації та кластеризації.

Перспективою для подальших досліджень є впровадження цих способів виявлення характеристик шкідливих зразків для проектування антивірусних продуктів, які використовують не лише сигнатурний підхід, але й можуть виявляти шкідливі зразки із функціями самоперетворення.

Перелік посилань

[1] P. O'kane, S. Sezer, K. McLaughlin, *Detecting obfuscated malware using reduced opcode set and optimised runtime trace*. Security informatics, Dec. 2016, 5:2 [Online]. Available: https://link.springer.com/article/ 10.1186 /s13388-016-0027-2#Sec6.

[2] Babak Bashari Rad, Maslin Masrom, *Metamorphic virus detection in Portable Executables using opcodes statistical feature*. Proceeding of the International Conference on Advance Science, Engineering and Information Technology, 14 - 15 January 2011, p 403-408 [Online]. Available: https://arxiv.org/pdf/ 1104.3229.pdf.

[3] E. Konstamtinou, *Metamorphic Virus: Analysis and Detection*. Technical Report RHUL-MA-2008-02 .-2008. [Online]. Available: https://www.ma.rhul.ac.uk/static/techrep/2008/RHUL-MA-2008-02.pdf.

[4] Structural similarity. Title from screen. [Online]. Available: https://en.wikipedia.org/ wiki/Structural_similarity.

[5] О. Єремізін, І. Стьопочкіна, *Перспективи використання нечіткого хешування в антивірусному захисті* // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні.-2016, №1(31).-С.80-85.

References

[1] P. O'kane, S. Sezer, K. McLaughlin, *Detecting obfuscated malware using reduced opcode set and optimised runtime trace.* Security informatics, Dec. 2016, 5:2 [Online]. Available: https://link.springer.com/article/ 10.1186 /s13388-016-0027-2#Sec6.

[2] Babak Bashari Rad, Maslin Masrom, *Metamorphic virus detection in Portable Executables using opcodes statistical feature.* Proceeding of the International Conference on Advance Science, Engineering and Information Technology, 14 - 15 January 2011, p 403-408 [Online]. Available: https://arxiv.org/pdf/ 1104.3229.pdf.

[3] E. Konstamtinou, *Metamorphic Virus: Analysis and Detection.* Technical Report RHUL-MA-2008-02 .-2008. [Online]. Available: https://www.ma.rhul.ac.uk/static/techrep/2008/RHUL-MA-2008-02.pdf.

[4] Structural similarity. Title from screen. [Online]. Available: https://en.wikipedia.org/wiki/Structural_similarity.

[5] O. Yeremizin, I. Stopochkina, *Perspektyvy vykorystannia nechitkoho kheshuvannia v antyvirusnomu zakhysti* // Pravove, normatyvne ta metrolohichne zabezpechennia systemy zakhystu informatsii v Ukraini.-2016, #1(31).-S.80-85.

Реферат

Кожокар Владислав; Стьопочкіна Ірина

Структурні закономірності еволюціонування метаморфного шкідливого ПЗ

На основі аналізу технік перетворення та особливостей функціонування шкідливого ПЗ метаморфного типу виділено характеристики, які можуть бути використані для класифікації та кластеризації шкідливого ПЗ із самоперетворенням. Встановлено, що спорідненість оригінала та нащадків можливо встановлювати за допомогою показників структурної подібності та за допомогою показників подібності текстів, які слід застосовувати в комплексі із кількісним аналізом на основі опкодів. Встановлено, що між батьком і першим нащадком є найвища ступінь несхожості, але нащадки не настільки суттєво несхожі між собою внаслідок специфіки метаморфних перетворень.

Кожокар Владислав; Степочкина Ирина

Структурные закономерности эволюционирования метаморфного вредоносного ПО

На основании анализа техник преобразования и особенностей функционирования вредоносного ПО метаморфного типа выделены характеристики, которые могут быть использованы для классификации и кластеризации вредоносного ПО с самопреобразованием. Установлено, что родственность оригинала и потомков возможно выявлять при помощи показателей структурного соответствия и при помощи показателей подобия текстов, которые следует применять в комплексе с количественным анализом на основе опкодов. Для реализации этих способов разработано соответствующее ПО. Установлено, что между отцом и первым потомком – наивысшая степень непохожести, но потомки не настолько непохожи между собой вследствие специфики метаморфных преобразований.

Kozhokar Vladyslav; Stopochkina Iryna

Structural patterns in metamorphic malware evolution

Based on the analysis of the evolution technique and the peculiarities of the functioning of the metamorphic malicious software, the characteristics that can be used for the classification and clustering of malicious software with self-transformation are highlighted. It has been established that the affinity of the original and the descendants can be established using structural similarity index and using similarity indicators of texts, which should be used in conjunction with quantitative analysis on the basis of opcodes. It is established that between the father and the first descendant is the highest degree of dissimilarity, but the descendants are not so much different from each other due to the specificity of metamorphic transformations.

Відомості про авторів

Стьопочкіна Ірина Валеріївна

Освіта: Вища (2001).

Науквий ступінь: Кандидат технічних наук (2005).

Місце роботи: Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського».

Область знань: Інформаційна безпека.

Наукові інтереси: Математичне моделювання, інформаційна безпека.

Email: *Iryna.styopochkina@gmail.com*

Кожокар Владислав Юрійович

Освіта: Вища (2017), студент магістратури КПІ ім. Ігоря Сікорського.

Область знань: Інформаційна безпека.

Наукові інтереси: Розробка програмного забезпечення, інформаційна безпека.

Email: *vladislav.kozhokar@gmail.com*

УДК: 004.056

ІДЕНТИФІКАЦІЯ ЗАГРОЗ НЕСАНКЦІОНОВАНОГО ДОСТУПУ ДО КОНФІДЕНЦІЙНИХ МЕРЕЖЕВИХ РЕСУРСІВ

Кец Дмитро; Присяжний Дмитро; Салієва Ольга
Вінницький національний технічний університет

IDENTIFYING THE THREAT OF UNPASSED ACCESS TO CONFIDENTIAL NETWORK RESOURCES

Kets Dmytro; Prysiazhnyi Dmytro; Saliieva Olha
Vinnytsia National Technical University

Анотація: **Розглянуто існуючі атаки на конфіденційні мережеві ресурси і способи їх виявлення, а також запропоновано метод і алгоритм ідентифікації загроз несанкціонованого доступу, що базується на аналізі фактичних даних об'єму мережевого трафіку. У роботі представлено тестування розробленого алгоритму, яке показало високу точність виявлення аномальної мережевої активності.**
Ключові слова: **Захист від несанкціонованого доступу, атаки на мережеві ресурси, ідентифікація загроз, прогнозування мережевих запитів, аномалії мережевої активності.**
Summary: **The existing attacks on confidential network resources and ways of their detection are considered, as well as the method and algorithm of identification of threats of unauthorized access, which is based on the analysis of actual data volume network traffic. The work presented the testing of the developed algorithm, which showed high accuracy of detection of abnormal network activity.**
Keywords: **Protection against unauthorized access, attacks on network resources, identification of threats, prediction of network requests, anomalies of network activity.**

Вступ

З позиції інформаційної безпеки велику загрозу доступності веб-ресурсу створює сканування автоматизованими ресурсами [1] – [26]. Метою таких сканувань є частково або повністю паралізувати роботу вузла, що атакується. Оскільки це спричиняє зниження якості отримуваних користувачем послуг, чи взагалі унеможливлює отримання будь-яких послуг, то важливим завданням є розробка методів для забезпечення захисту від сканування. У зв'язку з цим доцільним також є удосконалення методів ідентифікації, що може забезпечити підвищення надійності роботи веб-ресурсу за рахунок виявлення атаки до того, як вона вплине на працездатність.

Аналіз існуючих методів вирішення проблеми

Загалом виділяють два методи виявлення DoS-атак – аналіз інформаційного мережевого потоку і аналіз журналів реєстрації операційної системи або додатків [3]. Перший підхід до виявлення атак є більш ефективним з причини реагування у реальному масштабі часу. Тому основні дослідження наразі спрямовані на розробку способів і процедур виявлення атак у мережевому трафіку.

Тут основним завданням є ідентифікація шкідливого трафіку. Більшість атак у даний час важко відрізнити від звичайних дій користувачів. У той же час, зворотнє твердження так само справедливе – часто діяльність користувачів викликає ефекти, ідентичні ефекту від проведення розподіленої атаки відмови в обслуговуванні. Атака визначається як неприродна і помітна зміна статистичних властивостей досліджуваного трафіку.

Визначення профілю активності. Профіль активності визначається в результаті аналізу інформації із заголовків

мережевих пакетів. На основі ідентичних параметрів полів заголовку (таких як адреса, порт, протокол) створюється профіль активності – середній рівень активності окремо взятого мережевого потоку. Рівень активності виражається у вигляді періоду часу, що пройшов між надходженнями пакетів з ідентичними параметрами. Таким чином, загальна картина мережевої активності може бути представлена у вигляді суми рівнів активності усіх вхідних і вихідних з'єднань.

У результаті атака може бути виявлена у таких випадках:

– збільшення рівня активності кластерів, тобто зростання активності атакуючих вузлів (це може виражатися у зростанні швидкості передавання, зменшенні OFF-періодів бездіяльності);

– збільшення загальної кількості кластерів, що може бути визначено як початок здійснення розподіленої атаки

Точки зміни стану. Трафік фільтрується у залежності від адреси, порту або протоколу і результуючим кластерам ставиться у відповідність безліч станів у різні моменти часу. Приклад – алгоритм Cusum [10] (алгоритм інтегральних сум), що оперує з послідовними наборами даних. Для виявлення DoS-атаки визначається відхилення середніх значень параметрів трафіку.

Хвильовий аналіз (вейвлет-аналіз) [11]. Спосіб розглядає вхідні сигнали як спектральні компоненти. На відміну від аналізу Фур'є, хвильовий аналіз враховує тимчасові характеристики. Алгоритм розділяє вхідний сигнал на аномальні складові і зовнішній шум. В ідеалі шум і змістова складова повинні бути рознесені за спектром частот. На основі аналізу спектру робиться висновок про наявність аномалій.

Проблеми способів виявлення DoS-атак:

– **Проблема варіювання умов тестування.** Більшість способів виявлення розроблені і вивчені комплексно. Проведення комплексних досліджень ускладнено і вимагає великих часових витрат.

– **Проблема оцінювання природної мережевої активності.** Виявлення атак прив'язане до статистичних властивостей природної мережевої активності. Моделі атаки, що використовуються в розглянутих підходах, складають малу частину від загальної кількості можливих атак.

– **Проблема визначення параметрів детектування.** Кожен із способів виявлення атак має певний набір параметрів, таких як спосіб розбиття трафіку на кластери, значення порогів, рівень фільтру у хвильовому методі та інші. Визначення значень цих параметрів достатньо ускладнено і залежить від конкретних умов, в яких функціонує система виявлення атак.

– **Проблема раннього прогнозу атаки.** Для сучасних систем мало виявити атаку слід мати механізми її прогнозування (і ранньої протидії).

Розглянуті методи виявлення атак не мають таких можливостей, щоб виконати кластеризацію трафіку. Необхідно цей трафік (з атакуючими пакетами і за досить суттєвий проміжок часу) у вигляді файлу вже мати. Деяким типам (невідомих) атак не існує протидії в існуючій системі захисту. Тому проблема раннього прогнозу (навіть з великою ймовірністю помилкової загрози) досить істотна для систем виявлення атак.

Таким чином, проблема виявлення DoS-атак на основі аналізу мережевого трафіку у даний час є досить актуальною.

Постановка задачі

Для вирішення задачі підвищення захисту веб-ресурсів від сканування автоматизованими ресурсами необхідно розробити метод та алгоритм вдосконаленої ідентифікації, які містили б роботу із збору та аналізу мережевого трафіку, а також прогнозування кількості запитів на конкретний день або годину.

Для ефективного вирішення поставленої задачі необхідно обрати оптимальні технології та методи.

Ідентифікація загроз несанкціонованого доступу до мережевих ресурсів на основі аналізу та прогнозування трафіку

Умовно технологія збору інформації про мережеву активність класифікується таким чином [13]:

– моніторинг каналів (здійснюється на 2-му рівні моделі OSI),

– облік трафіку (здійснюється на 3-му і 4-му рівнях моделі OSI),

– перехоплення і аналіз даних, що передаються (здійснюється на 2-7 рівнях моделі OSI).

Моніторинг та управління мережевими пристроями традиційно здійснюється за допомогою протоколу Simple Network Management Protocol (SNMP)

Найбільш відомою технологією обліку трафіку є протокол NetFlow корпорації Cisco. Протокол NetFlow дозволяє пристроям Cisco передавати дані про трафік, що проходить через даний пристрій, на будь хост у мережі де ці дані можуть накопичуватися, зберігатися у певному виді і відповідно відображатися.

Сьогодні практично будь-який керований комутатор забезпечений можливістю перехоплення і аналізу протоколів, що проходять через його порти. На практиці зустрічаються різні назви даної технології: Port Monitoring, Port Mirroring або Switch Port Analyzer (SPAN). У рамках цієї технології забезпечується конфігурація окремого порту, в який буде потрапляти необхідний для аналізу трафік з інших портів, що у звичайному режимі комутації не допускається.

Аналіз та вивчення трафіку через інтерфейси обладнання забезпечується за допомогою мережевих аналізаторів, основна функція яких полягає у декодуванні і відображенні вмісту захоплених пакетів. Найбільшого поширення набуло програмне забезпечення, що дозволяє перехоплювати мережеві пакети на інтерфейсах робочих станцій і серверів [12]. У поєднанні з апаратними засобами (SPAN) вони представляють потужні засоби аналізу мережевої активності.

Значення кількості запитів до веб-ресурсу за одиницю часу можуть бути розглянуті як впорядкована у часі послідовність, що складається зі значень різної величини. Тобто, кількість запитів може бути представлена у вигляді часового ряду. Часовий ряд – це послідовні виміри, впорядковані у невипадкові моменти часу [11]. Аналіз часових рядів базується на припущенні, що послідовні значення у файлі даних спостерігаються через рівні проміжки часу.

З метою ідентифікації ситуації у мережі є необхідним проведення статистичного аналізу часового ряду. Для підвищення точності результатів потрібно відкинути аномально високі і аномально низькі значення. Для цього необхідно обчислити значення середнього арифметичного f і стандартного відхилення S.

При математичному описі часовий ряд, що аналізується завжди розглядається як одна з таких складових або сума декількох з них. Якщо в часовому ряду проявляється тривала тенденція зміни деякого показника, то вважається, що має місце тренд. Таким чином, під трендом розуміється зміна, що визначає загальний напрямок розвитку, основну тенденцію часових рядів [17].

Для того щоб виключити з трафіку випадкові коливання, необхідно виконати згладжування даних. Суть різних прийомів згладжування зводиться до заміни фактичних рівнів часового ряду розрахунковими рівнями, які в меншій мірі схильні до коливань.

Методи згладжування можна умовно розділити на два класи, що опираються на аналітичний та алгоритмічний підхід.

Аналітичний підхід заснований на припущенні, що дослідник може задати загальний вигляд функції, яка описує регулярну, невипадкову складову. Наприклад, на основі візуального та змістовного аналізу динаміки часового ряду передбачається, що трендова складова може бути описана за допомогою показникової функції. Тоді на наступному

етапі буде проведено статистичне оцінювання невідомих коефіцієнтів моделі, а потім визначені згладжені значення рівнів часового ряду шляхом підстановки відповідного значення часового параметру в отримане рівняння (задане в явному аналітичному вигляді).

Також для усунення випадкових коливань використовується метод короткострокової центрованої рухомої (ковзаючої) середньої ряду даних.

Алгоритм згладжування за даним методом може бути представлений у вигляді такої послідовності кроків:

1. Визначається довжина інтервалу згладжування l, що включає в себе n послідовних рівнів ряду $(l < n)$.

2. Весь період спостереження розбивається на ділянки. При цьому інтервал згладжування якби ковзає по ряду з кроком, рівним l.

3. Розраховуються середні арифметичні з рівнів ряду, що утворюють кожну ділянку

4. Фактичні значення ряду, що стоять у центрі кожної ділянки, замінюються на відповідні середні значення.

При цьому зручно брати довжину інтервалу згладжування l як непарне число: $l = 2p + 1$, тому що в цьому випадку отримані значення рухомої середньої припадають на середній член інтервалу.

Дані, які беруться для розрахунку середнього значення, називаються активною ділянкою згладжування.

При використанні рухомої середньої з довжиною активної ділянки $l = 2p + 1$ перші і останні p рівнів ряду згладити не можна, тому їх значення втрачаються. Очевидно, що втрата значень останніх точок є істотним недоліком, так як для прогнозу останні дані мають найбільшу інформаційну цінність.

Розглянемо один з прийомів, що дозволяють відновити втрачені значення часового ряду при використанні даного методу згладжування. Для цього необхідно обчислити середній абсолютний приріст на останній активній ділянці:

$$\overline{\Delta y} = \frac{y_{t+p} - y_{t-p}}{l - 1}$$

де l – довжина активної ділянки;

y_{t+p} – значення останнього рівня на активній ділянці;

y_{t-p} – значення першого рівня на активній ділянці;

$\overline{\Delta y}$ – середній абсолютний приріст на останній активній ділянці.

Після чого необхідно отримати p згладжених значень в кінці часового ряду шляхом послідовного додавання середнього абсолютного приросту до останнього згладженого значення.

Аналогічну процедуру можна реалізувати для оцінювання перших рівнів часового ряду.

Після виключення з ряду динаміку трафіку випадкових коливань можна виконувати прогнозування даних.

Прогнозування мережевого трафіку здійснюватиметься на основі статистичних методів. Статистичні методи використовуються для прогнозування різноманітних коливань показників. Прогноз – це передбачення майбутнього на основі наукових методів (можливих станів об'єкта у майбутньому) [19]. Статистичні методи дозволяють на основі зібраної за визначений час статистики виділяти закономірності, приховані на фоні випадковостей, робити обґрунтовані прогнози і оцінювати ймовірності.

При застосуванні статистичних методів можна виділити такі етапи:

– планування статистичного дослідження;

– організація збору необхідних статистичних даних за оптимальною або раціональною програмою (планування вибірки, створення організаційної структури і підбір команди статистиків, підготовка кадрів, які займатимуться збиранням даних, а також контролерів даних тощо);

– безпосереднє збирання даних та їх фіксація на тих чи інших носіях (з

контролем якості і відкиданням помилкових даних);

– первинний опис даних (розрахунок різних вибіркових характеристик, функцій розподілу, непараметричних оцінок щільності, побудова гістограм, кореляційних полів, різних таблиць і діаграм тощо);

– оцінювання тих чи інших числових або нечислових характеристик і параметрів розподілів (наприклад, непараметричне інтервальне оцінювання коефіцієнта варіації або відновлення залежності між відгуком і факторами, тобто оцінювання функції);

– перевірка статистичних гіпотез (іноді їх ланцюжків – після перевірки попередньої гіпотези приймається рішення про перевірку тієї чи іншої подальшої гіпотези);

– більш поглиблене вивчення, тобто застосування різних алгоритмів багатовимірного статистичного аналізу, алгоритмів діагностики та побудови;

– класифікація, статистика нечислових та інтервальних даних, аналіз часових рядів тощо;

– перевірка стійкості отриманих оцінок і висновків щодо допустимих відхилень вихідних даних і передумов використовуваних ймовірнісно-статистичних моделей;

– застосування отриманих статистичних результатів у прикладних цілях, наприклад, для побудови прогнозів;

– складання підсумкових звітів.

Для прогнозування часових рядів зазвичай використовуються такі методи прогнозування:

– «наївні» моделі прогнозування;

– методи Хольта і Брауна;

– метод Вінтерса;

– регресійні методи прогнозування;

– методи Бокса-Дженкінса;

– нейромережеві моделі.

У даній роботі для прогнозування використано алгоритм з використанням кривих зростання, який враховує тренд даних, а також є стійким до випадкових коливань. Допустимі результати прогнозу досягаються при невеликій кількості даних і тому його доцільно застосувати для реалізації поставленої задачі.

Правильно обрана модель кривої зростання повинна відповідати характеру зміни тенденції досліджуваного явища. Крива росту дозволяє отримати вирівнені або теоретичні значення рівнів динамічного ряду. Це ті рівні, які спостерігалися б у разі повного збігу динаміки явища з кривою зростання.

Прогнозування на основі моделі кривої зростання базується на екстраполяції, тобто на продовженні в майбутнє тенденції, що спостерігалася в минулому.

Алгоритм розробки прогнозу з використанням кривих зростання включає в себе наступні етапи:

– вибір однієї або декількох кривих, форма яких відповідає характеру зміни часового ряду;

– перевірка адекватності обраних кривих прогнозованого процесу, оцінка точності моделей і остаточний вибір кривої зростання;

– оцінка параметрів кривої;

– розрахунок прогнозу.

До 1-го класу відносяться функції, що використовуються для опису процесів з монотонним характером тенденції розвитку і відсутністю меж зростання. До 2-го класу відносяться криві, що описують процес, який має межу зростання у досліджуваному періоді. Функції, які належать до 2-го класу, називаються кривими насичення. Якщо криві насичення мають точки перегину, то вони відносяться до 3-го типу кривих росту – до S-подібних кривих. [11]

Серед кривих зростання 1-го типу, насамперед, варто виділити клас поліномів:

$$\hat{y}_t = a_0 + a_1 t + a_2 t^2 + ... + a_p t^p,$$

де a_i $(i = 0, 1, ..., p)$ – параметри многочлена,

t – незалежна змінна, $t = 1, 2, ..., n$.

Зазвичай в дослідженнях застосовуються поліноми не вище третього порядку. Використовувати для визначення тренда поліноми високих ступенів не доцільно, оскільки отримані таким чином апроксимуючі

функції будуть відображати випадкові відхилення (що суперечить змісту тенденції).

Поліном першого ступеня $\hat{y}_t = a_0 + a_1 t$ на графіку зображується прямою і використовується для опису процесів, що розвиваються у часі рівномірно.

Поліном другого ступеня $\hat{y}_t = a_0 + a_1 t + a_2 t^2$ застосовується у тих випадках, коли процес розвивається рівноприскорено. Як відомо, якщо параметр $a_2 > 0$, то гілки параболи спрямовані вгору, якщо ж $a_2 < 0$, то вниз. Параметри a_0 і a_1 не впливають на форму параболи, а лише визначають її положення.

Поліном третього ступеня має вигляд:

$$\hat{y}_t = a_0 + a_1 t + a_2 t^2 + a_3 t^3.$$

У цього полінома знак приросту ординат може змінюватися один або два рази.

Відмінна риса поліномів – відсутність в явному вигляді залежності приростів від значень ординат (y_t).

Після того як, сформована трендова модель, необхідно провести її оцінку адекватності і точності.

Трендова модель $\hat{Y}_t$ конкретного часового ряду Y_t, вважається адекватною, якщо правильно відображає систематичні компоненти часового ряду. Для виконання цієї вимоги необхідно, щоб залишкова компонента: $\varepsilon_t = \hat{Y}_t - Y_t$, де $t = 1, 2, \ldots, n$ задовольняла властивостям випадкової компоненти часового ряду, а саме [18]:

– випадковість коливань рівнів залишкової послідовності;

– відповідність розподілу випадкової компоненти нормальному закону розподілу;

– рівність математичного сподівання випадкової компоненти нулю;

– незалежність значень рівнів випадкової компоненти.

Критерієм для перевірки випадковості коливань рівнів залишкової послідовності може служити критерій піків (поворотних точок) [19]. Згідно з цим критерієм рівень послідовності ε_t вважається максимумом, якщо він більше двох рівнів, що стоять поруч, і мінімумом, якщо він менше обох сусідніх рівнів. В обох випадках ε_t вважається поворотною точкою.

Позначимо через p – загальне число поворотних точок для залишкової послідовності ε_t.

У випадковій вибірці математичне сподівання числа точок повороту $\overline{p}$ і дисперсія σ_t^2 виражаються формулами [19]:

$$\overline{p} = \frac{2}{3}(n-2),$$

$$\sigma_t^2 = \frac{16n - 29}{90}.$$

Критерієм випадковості з 5%–м рівнем значущості, тобто з довірчою ймовірністю 95%, є виконання нерівності:

$$p > \left[\overline{p} - 1.96\sqrt{\sigma_t^2} \right],$$

де квадратні дужки означають цілу частину числа.

Якщо нерівність не виконується, то трендова модель вважається неадекватною.

Для перевірки нормальності закону розподілу випадкової компоненти застосовується, наприклад, *RS*-критерій. Цей критерій чисельно дорівнює відношенню розмаху варіації випадкової величини *R* до стандартного відхилення *S*, де *R* і *S* обчислюються за формулами [20]:

$$R = \varepsilon_{\max} - \varepsilon_{\min},$$

$$S = \sqrt{\frac{\sum \varepsilon_t^2}{n-1}}.$$

Обчислене значення *RS*-критерію порівнюється з табличними (критичними) нижньою і верхньою межами даного відношення, і якщо це значення не потрапляє в інтервал між критичними межами, то за даним рівнем значущості гіпотеза про нормальність розподілу відкидається; в іншому випадку – гіпотеза приймається.

Перевірка рівності нулю математичного сподівання випадкової компоненти, якщо вона розподілена за нормальним законом, здійснюється на основі *t*-критерію Стьюдента. Розрахункове значення цього критерію задається формулою [10]:

$$t = \frac{\bar{\varepsilon} - 0}{G}\sqrt{n},$$

де $\bar{\varepsilon}$ – середнє арифметичне значення рівнів залишкової послідовності ε_t;

G – середньоквадратичне відхилення для цієї послідовності.

Якщо розрахункове значення t менше табличного значення t_a статистики Стьюдента із заданим рівнем значущості і числом ступенів свободи $n-1$, то гіпотеза про рівність нулю математичного очікування випадкової послідовності приймається; в іншому випадку ця гіпотеза відкидається і трендова модель вважається неадекватною.

Перевірка незалежності значень рівнів випадкової компоненти, тобто перевірка відсутності істотної автокореляції в остаточній послідовності, може здійснюватися по ряду критеріїв, найбільш поширеним з яких є *d*-критерій Дарбіна-Уотсона. Розрахункове значення цього критерію визначається за формулою [18]:

$$d = \frac{\sum(\varepsilon_t - \varepsilon_{t-1})^2}{\sum \varepsilon_t^2}.$$

Розрахункове значення критерію d в інтервалі від 2 до 4 свідчить про негативну зв'язку. В цьому випадку його необхідно перетворити за формулою $d' = 4 - d$ і у подальшому використовувати значення d'.

Розрахункове значення критерію d (або d') порівнюється з верхнім і нижнім критичними значеннями статистики Дарбіна-Уотсона. Якщо розрахункове значення критерію d більше верхнього табличного значення, то гіпотеза про незалежність рівнів залишкової послідовності, тобто про відсутність в ній автокореляції, приймається. Якщо значення d менше нижнього табличного значення, то гіпотеза відкидається і модель неадекватна. Якщо значення d знаходиться між верхнім і нижнім значеннями і включає самі ці значення, то вважається, що немає достатніх підстав зробити той чи інший висновок і необхідні подальші дослідження, наприклад, за більшою кількістю спостережень.

Висновок про адекватність трендової моделі робиться у тому випадку, якщо всі чотири зазначені перевірки властивостей залишкової послідовності дають позитивний результат.

Для адекватної трендової моделі необхідно провести перевірку її точності. Точність моделі характеризується величиною відхилення виходу моделі від реального значення модельованої змінної. Для даного показника, представленого часовим рядом, точність визначається як різниця між значенням фактичного рівня часового ряду і його оцінкою, отриманою розрахунковим шляхом з використанням моделі [21].

В якості статистичного показника точності тренду застосовується середня відносна помилка апроксимації, що розраховується за формулою [22]:

$$\bar{\varepsilon}_{відн} = \frac{1}{n}\sum_{t=1}^{n}\left|\frac{f_t - y_t}{f_t}\right| \cdot 100\%,$$

де f_t – значення рівня початкового ряду;

y_t – значення рівня тренду.

Значення помилки у межах 5 – 7% свідчить про точність тренду.

Після перевірки адекватності і точності обраної кривої тренду необхідно оцінити її параметри. Оцінки параметрів у моделі визначаються методом найменших квадратів. Суть цього методу полягає в знаходженні таких параметрів, при яких сума квадратів відхилень розрахункових значень рівнів від фактичних значень була б мінімальною. Таким чином, ці оцінки знаходяться в результаті мінімізації виразу:

$$\sum_{t=1}^{n}\left(y_t - \hat{y}_t\right)^2 \to \min,$$

де y_t – фактичне значення рівня часового ряду;

$\hat{y}_t$ – розраховане значення;

n – довжина часового ряду.

Результатом мінімізації виразу є система лінійних рівнянь, розв'язання якої дозволяє обчислити оцінки коефіцієнтів, що шукаються.

Система рівнянь для оцінювання параметрів прямої (полінома першого ступеня $\hat{y}_t = a_0 + a_1 t$) має вигляд:

$$\begin{cases} \sum y_t = a_0 \cdot n + a_1 \sum t, \\ \sum y_t \cdot t = a_0 \sum t + a_1 \sum t^2. \end{cases}$$

Розв'язання системи відносно параметрів, що визначається на такі вирази:

$$a_0 = \frac{\sum y_t}{n} - a_1 \frac{\sum t}{n},$$

$$a_1 = \frac{\sum y_t t - \frac{\sum y_t}{n} \cdot \sum t}{\sum t^2 - \frac{(\sum t)^2}{n}}.$$

Для параболи отримаємо аналогічну систему рівнянь:

$$\begin{cases} \sum y_t = a_0 \cdot n + a_1 \sum t + a_2 \sum t^2, \\ \sum y_t \cdot t = a_0 \sum t + a_1 \sum t^2 + a_2 \sum t^3, \\ \sum y_t \cdot t^2 = a_0 \sum t^2 + a_1 \sum t^3 + a_2 \sum t^4. \end{cases}$$

Система містить три рівняння, які дозволяють знайти оцінки трьох невідомих коефіцієнтів a_0, a_1, a_2. Вирази для розрахунку можна спростити шляхом перенесення початку координат у середину ряду динаміки. Це дозволяє спростити самі рівняння, а також зменшити абсолютні значення величин, які враховуються при розрахунках.

Якщо до перенесення початку координат значення t становило 1, 2, 3, …, то після перенесення:

– для парного числа членів ряду t = …, -5, -3, -1, 1, 3, 5, …;

– для непарного числа членів ряду t = …, -3, -2, -1, 0, 1, 2, 3, ….

Такий підхід значно спрощує системи рівнянь.

Після перенесення початку координат у середину ряду динаміки оцінки параметрів відповідних поліномів визначаються за допомогою спрощених виразів.

Для лінійної залежності вирази мають такий вигляд:

$$a_0 = \frac{\sum y_t}{n},$$

$$a_1 = \frac{\sum y_t \cdot t}{\sum t^2}.$$

Обчислення коефіцієнтів для параболічної залежності можна виконати за виразами:

$$a_0 = \frac{\sum y_t}{n} - \frac{\sum t^2}{n}\left[\frac{n\sum y_t \cdot t^2 - \sum t^2 \sum y_t}{n\sum t^4 - (\sum t^2)^2}\right],$$

$$a_1 = \frac{\sum y_t \cdot t}{\sum t^2},$$

$$a_2 = \frac{n\sum y_t \cdot t^2 - \sum t^2 \sum y_t}{n\sum t^4 - (\sum t^2)^2}.$$

У формулах додавання проводиться за t, отриманому після перенесення початку координат у середину ряду динаміки.

Отримані значення коефіцієнтів підставляються у рівняння полінома відповідного ступеня і розраховується прогнозоване значення величини.

Для оцінювання точності отриманих значень скористаємося показником APE – середньою абсолютною помилкою у відсотках (absolute percentage error), яка розраховується за формулою [23]:

$$APE_t = \left|\frac{y_t - \hat{y}_t}{y_t}\right| \cdot 100\%.$$

Значення оцінки APE не повинно виходити за межі допустимих значень для конкретної кількості хостів у мережі.

Було розроблено алгоритм підвищення захисту веб-ресурсів від сканування автоматизованими ресурсами шляхом вдосконаленої ідентифікації.

Для цього було розглянуто існуючі атаки на веб-ресурси, зокрема, атаки типу «відмова в обслуговуванні», а також методи їх виявлення.

Використання цих методів, незважаючи на переваги, має також і ряд загальних недоліків. У зв'язку з цим було запропоновано алгоритм, що полягає у захисті веб-ресурсів шляхом аналізу кількості запитів до веб-ресурсу, виконання прогнозування на основі отриманих даних і порівняння прогнозу з фактичним значенням.

Етапами реалізації даного алгоритму є:

– збір даних про динаміку трафіку;

– розрахунок середньоарифметичного значення та його порівняння з фактичними даними;

– розрахунок оцінки стандартного відхилення випадкової величини;

– визначення верхнього та нижнього порогових значень;

– згладжування ряду;

– вибір кривої тренду, форма якої відповідає характеру зміни ряду;

– оцінка адекватності тренду;

– перевірка точності тренду шляхом розрахунку помилки апроксимації;

– складання системи рівнянь методом найменших квадратів;

– розрахунок оцінок параметрів кривої тренду;

– безпосереднє виконання прогнозу;

– обчислення середньої абсолютної помилки;

– порівняння фактичного значення кількості запитів з прогнозованим;

– при необхідності блокування IP-адреси несанкціонованого користувача.

Методом найменших квадратів були розраховані коефіцієнти рівняння, на основі яких виконаний прогноз. Помилка прогнозу становить 3,71 – 4,54 % і знаходиться в межах допустимих значень. Таким чином, порівнюючи фактичні значення з прогнозованими можна виявити аномальну активність і заблокувати IP-адресу.

Висновки

Розглянуто технології та методи збору інформації про трафік, аналізу та попередньої обробки зібраних даних і прогнозування на основі цих даних.

Для ефективного вирішення поставленої задачі було запропоновано метод і розроблено алгоритм підвищення захисту веб-ресурсів від сканування автоматизованими ресурсами шляхом вдосконаленої ідентифікації. Також було запропоновано метод прогнозування кількості запитів у мережевому трафіку.

Перелік посилань

[1] И. В. Котенко, М. В. Степашкин, Е. В. Дойникова, *Анализ защищенности автоматизированных систем с учетом социоинженерных атак* // Проблемы информационной безопасности. Компьютерные системы. 2011 – №3 – С.40–57.

[2] Mahammad-oglu Alguliev Rasim, Irada Yavar-kizi Alakbarova, *Порівняльний аналіз інформаційних атак в інтернеті* / Інформаційні технології та комп'ютерна інженерія – Вінниця: Видавництво Вінницького національного технічного університету, 2010. – Том 3 – № 19.

[3] Do-Yoon Ha, *Design and Implementation if SIP-aware DDoS Attack Detection System* / Do-Yoon Ha, Chang-Yong Lee, Hyun-Cheol Jeong // Advances in Information Sciences – 2010 – Vol.2 №4.

[4] А. Н. Марьенков, *Повышение безопасности компьютерных систем и сетей на основе анализа сетевого трафика* / А.Н. Марьенков, И.М. Ажмухамедов // *Инфокоммуникационные технологии – 2010 – №3 – Т.8.* с.106-108.

[5] В. Н. Олифер, Н. А. Олифер *Компьютерные сети. Принципы. Технологии, протоколы* – 4–е изд. – Спб: Питер, 2010. – 944 с.

[6] A. M. Sukhov, *Active flows in diagnostic of troubleshooting on backbone links* / A. A. Galtsev, A. M. Sukhov, D. I. Sidelnikov, A. P. Platonov, M. V. Strizhov // Journal of High Speed Networks . – 2011. – Vol. 18. – №. 1. – P. 69-81.

[7] Е. И. Чернышевская, *Метод обеспечения гарантированого качества обслуживания в IP-сетях* / Е.И. Чернышевская, И.Ю.Селянина // *«Век качества» – №6 – 2010.* – с.70-72.

[8] D. Serpanos, *Architecture of Network Systems Computer* / D. Serpanos, W. Tilman // Security Magazine, 2011. – P. 44-45.

[9] Б. Ю. Лемешко**,** *Статистический анализ данных, моделирование и исследование вероятностных закономерностей. Компьютерный подход: монография* / Б. Ю. Лемешко, С. Б. Лемешко, С. Н. Постовалов, Е. В. Чимитова – Новосибирск, Изд–во НГТУ, 2011 – 888 с.

[10] В. І. Романчук, *Дослідження імовірнісних властивостей трафіку корпоративної мультисервісної мережі* / В. І. Романчук, О. А. Лаврів, В. В. Червенець, Р. І. Бак // Радіоелектроніка та телекомунікації : [збірник наукових праць] / відповідальний редактор Б. А. Мандзій. – Львів : Видавництво Львівської політехніки, 2011. – с. 128–134. – (*Вісник / Національного університету «Львівська політехніка» ; № 705*).

[11] В. Н. Афанасьев**,** *Анализ временных рядов и прогнозирование: учебник для студентов высших учебных заведений* / В. Н. Афанасьев, М. М. Юзбашев – 2-е изд., перераб. и доп. – Москва: Финансы и статистика, 2010. – 317 с.

[12] S. Hummel**,** *Network Performance and Optimization Guide: The Essential Network Performance* / S. Hummel // *Create-Space Independent Publishing. – Toronto, 2013*. – P. 111-113.

[13] B. G. Ibrahimov, *Research and estimation characteristics of terminal equipment a part of multiservice communication networks* / B. G. Ibrahimov // *Automatic Control and Computer Sciences. – 2010. – Vol.48. – No.6.* – P. 54-59.

[14] Н. М. Іванущак, *Математичні моделі розвитку структур комп'ютерних мереж: автореферат дисертації на здобуття наукового ступеня кандидата технічних наук* / Н. М. Іванущак // *Національний університет «Львівська політехніка» – Львів, 2013.* – 20 с.

[15] С. Н. Степанов, *Основы телетрафика мультисервисных сетей* / С. Н. Степанов – Москва.: Эко–Трендз, 2010. – 256 с.

[16] Г. І. Купалова, *Теорія економічного аналізу*. Навчальний посібник. – К.: Знання, 2008. – 639 с.

[17] Л. І. Панасенко, Г. П. Голубкина, *Теорія економічного аналізу*: Навчальний посібник. – К.: Вид.–поліграфічний центр "Київський університет", 2007. – 150 с.

[18] В. Г. Минашкин, *Бизнес–статистика и прогнозирование*: учебно–практическое пособие / В. Г. Минашкин, Н. А. Садовникова, Р. А. Шмойлова – Москва : Изд. центр ЕАОИ, 2010. – 254 с.

[19] В. М. Дубовой, *Прогнозування доцільної кількості повторень циклічного технологічного процесу* / В. М. Дубовой, І. В. Пилипенко, Р. С. Стець // Вінниця: Видавництво Вінницького національного технічного університету (Вісник ВПІ), 2015. – ст.86-91.

[20] Н. В. Ковтун, *Теорія статистики:* Курс лекцій, практикум. – К.: Імекс-ЛТД, 2012. – 276 с.

[21] Ю. А. Крюков, Д. В. Чернягин, *Модель прогнозирования значений трафика* // Информационные технологии и вычислительные системы – 2011 – №2 – с.41–49.

[22] В. А. Петрук, Г. Г. Кашканова, *Ймовірнісно-статистичні моделі та статистична оцінка рішень.* Навчальний посібник – Вінниця: УНІВЕРСУМ-Вінниця, 2006 – 131 с.

[23] Е. Г. Игнатенко, И. В. Дегтяренко, Н. В. Червинская, И. Н. Яремко, *Методика краткосрочного прогнозирования трафика телекоммуникационных сетей.* – Збірник наукових праць ДонІЗТ. 2011 №28 – 102–107 с.

[24] П. І. Бідюк, *Аналіз часових рядів*: навчальний посібник / П. І. Бідюк, В. Д. Романенко, О. Л. Тимощук. – К. : Політехніка, 2010. – 317 с.

[25] А. Головін, *Виявлення DDoS-атак прикладного рівня шляхом використання моделі MapReduce* / Андрій Головін // Information Technology and Security : collection of research papers. – 2015. – Vol. 3, Iss. 2 (5). – Pp. 117–124. – Bibliogr.: 12 ref.

[26] Н. В. Багнюк, *Види DDoS-атак та алгоритм виявлення DDoS-атак типу flood-attack* / Н. В. Багнюк, В. М. Мельник, О. В. Клеха, І. А. Невідомський // Комп'ютерно-інтегровані технології: освіта, наука, виробництво. – 2015. – № 18. – С. 6–12.

References

[1] I. Kotenko, M. Stepashkin, E. Doinikova, *Analysis of the security of automated systems with allowance for socioengineering attacks* // Problems of information security. Computer systems. 2011 - No. 3 - pp. 40-57.

[2] Mahammad-oglu Alguliev Rasim, Irada Yavar-kizi Alakbarova *Comparative Analysis of Information Attacks on the Internet* / Information Technologies and Computer Engineering - Vinnytsya: Vinnitsa National Technical University, 2010. - Vol. 3 - No. 19.

[3] Do-Yoon Ha, *Design and Implementation if the SIP-aware DDoS Attack Detection System* / Do-Yoon Ha, Chang-Yong Lee, Hyun-Cheol Jeong // Advances in Information Sciences - 2010 - Vol.2 No. 4.

[4] A. Marienkov *Improvement of security of computer systems and networks on the basis of analysis of network traffic* / A. N. Marienkov, I. M. Azhmukhamedov // Infocommunication technologies - 2010 - No. 3 - T.8. P.106-108

[5] V. Olifer, N. Olifer, *Computer networks. Principles Technologies, protocols* - 4th ed. - St. Petersburg: 2010. - 944 p.

[6] A. Sukhov, *Active flows in diagnostic of troubleshooting on backbone links* / A. A. Galtsev, A. M. Sukhov, D. I. Sidelnikov, A. P. Platonov, M. V. Strizhov // Journal of High Speed Networks. - 2011. - Vol. 18. - No. 1. P. 69-81.

[7] E. Chernyshevskaya, *Method of providing guaranteed quality of service in IP-networks* / E. И. Chernyshevskaya, I. Yu. Selyanina // "The Age of Quality" - No. 6 - 2010. - P. 70-72.

[8] D. Serpan, *Architecture of Network Systems Computer* / D. Serran, W. Tilman // Security Magazine, 2011. - P. 44-45.

[9] B. Lemeshko, *Statistical analysis of data, modeling and research of probabilistic regularities. Computer approach: monograph* / B. U. Lemeshko, S. B. Lemeshko, S. N. Postovalov, E. V. Chimitova - Novosibirsk, Publishing House of the National Technical University, 2011 - 888 p.

[10] V. Romanchuk, *Investigation of the probabilistic properties of the traffic of the corporate multiservice network* / V. I. Romanchuk, O. A. Lavrov, V. V. Cherventets, R. I. Bak // Radioelektronika i telekomunikatsiya: [collection of scientific works] / Responsible Editor B. A. Mandzii. - Lviv: Lviv Polytechnic Publishing House, 2011. - p. 128-134. - (Herald / *National University "Lviv Polytechnic", No. 705*).

[11] V. Afanasyev, *Analysis of time series and forecasting: a textbook for students of higher educational institutions* / V. Afanasyev, M. M. Yuzbashev - 2 ed., Pererab. And add - Moscow: Finance and Statistics, 2010. - 317 p.

[12] S. Hummel *Network Performance and Optimization Guide: The Essential Network Performance* / S. Hummel // Create-Space Independent Publishing. - Toronto, 2013. - P. 111-113.

[13] B. Ibrahimov, *Research and estimation characteristics of terminal equipment a part of multiservice communication networks* / B. G. Ibrahimov // Automatic Control and Computer Sciences. - 2010 - Vol.48. - No.6 - P. 54-59.

[14] N. Ivanushchak *Mathematical models of the development of computer network structures: dissertation dissertation for the degree of candidate of technical sciences* / N. M. Ivanushchak // National University "Lviv Polytechnic" - Lviv, 2013. – P. 20.

[15] S. Stepanov *Fundamentals of Teletraffic for Multiservice Networks* / S. N. Stepanov - Moscow: Eco-Trends, 2010. - 256 p.

[16] G. Kupalova *The theory of economic analysis. Tutorial.* - K .: Knowledge, 2008. - 639 p.

[17] L. Panasenko, G. Golubkina *Theory of Economic Analysis: Textbook.* - K .: Kind-Polygraphic Center "Kyiv University", 2007. - 150 p.

[18] V. Minashkin *Business statistics and forecasting: training manual* / V. Minashkin, N. A. Sadovnikova, R. A. Shmoilova - Moscow: Izd. EAOI Center, 2010. - 254 p.

[19] V. Dubovoy *Prediction of the appropriate number of repetitions of the cyclic technological process* / V. M. Dubova, I V Pilipenko, R. S. Stets // Vinnytsya: Publishing House of Vinnytsia National Technical University (*Vestnik VPI), 2015*. - p.86-91.

[20] Kovtun N. *Theory of Statistics: Course of lectures, workshop.* - K .: Imex-LTD, 2012. - 276 p.

[21] Yu. Kryukov, D. Chernyagin, *Model of forecasting of traffic values* // Information technologies and computing systems - 2011 - No.2 - p.41-49.

[22] V. Petruk, G. Kashkanova, *Probabilistic statistical models and statistical estimation of solutions. Training manual* - Vinnytsya: UNIVERSUM-Vinnytsia, 2006 - 131 p.

[23] E. Ignatenko, I. Degtyarenko, N. Chervinska, I. Yaremko, *Method of short-term forecasting of traffic of telecommunication networks. - Collection of scientific works DonIZT. 2011 №28* - 102-107 p.

[24] P. Bidyuk, *Analysis of time series: textbook* / P. I. Bidyuk, V. D. Romanenko, O. Timoschuk. - K.: Politechnika, 2010. - 317 p.

[25] A. Golovin, *Detection of application level DDoS attacks by using MapReduce model* / Andrei Golovin // Information Technology and Security: collection of research papers. - 2015. - Vol. 3, Iss. 2 (5). - pp 117-124. - Bibliogr .: 12 ref.

[26] N. Bagniuk, *Types of DDoS attacks and algorithm for detecting DDoS attacks such as flood-attack* / N. V. Bagniuk, V. M. Melnyk, O. V. Kleha, I. A. Nevidomsky // Computer-integrated Technology: education, science, production. - 2015. - No. 18. - P. 6-12.

Реферат

Кец Дмитро; Присяжний Дмитро; Салієва Ольга

Ідентифікація загроз несанкціонованого доступу до конфіденційних мережевих ресурсів

Важливим питанням при вирішенні завдань, пов'язаних з захистом мережевих ресурсів, є оперативне виявлення станів мережі, що призводять до втрати повної або часткової її працездатності, знищення, перекручення чи витоку інформації, що є наслідком відмов, збоїв випадкового характеру або результатом отримання зловмисником несанкціонованого доступу до мережевих ресурсів. Раннє виявлення таких станів дозволить своєчасно усунути їх причину, а також попередить можливі негативні наслідки. Тому для підвищення надійності роботи веб-ресурсу доцільним є удосконалення методів ідентифікації. Для вирішення даного питання в роботі було запропоновано метод і розроблено алгоритм ідентифікації загроз несанкціонованого доступу та представлено результати

тестування розробленого алгоритму. Отримані результати дозволяють стверджувати про високу точність виявлення аномальної мережевої активності.

Кец Дмитрий; Присяжный Дмитрий; Салиева Ольга

Идентификация угроз несанкционированного доступа к конфиденциальным сетевым ресурсам

Важным вопросом при решении задач, связанных с защитой сетевых ресурсов является оперативное выявление состояний сети, которые приводят к полной или частичной потере ее работоспособности, уничтожения, искажения или утечки информации, является следствием отказов, сбоев случайного характера или результатом получение злоумышленником несанкционированного доступа к сетевым ресурсам. Раннее выявление таких состояний позволит своевременно устранить их причину, а также предотвратит возможные негативные последствия. Поэтому для повышения надежности работы веб-ресурса целесообразным является усовершенствование методов идентификации. Для решения данного вопроса в работе был предложен метод и разработан алгоритм идентификации угроз несанкционированного доступа и представлено результаты тестирования разработанного алгоритма. Полученные результаты позволяют утверждать о высокой точности обнаружения аномальной сетевой активности.

Kets Dmytro; Prysiazhnyi Dmytro; Saliieva Olha

Identifying the threat of unpassed access to confidential network resources

An important issue when solving problems related to the protection of network resources is the operational detection of network conditions that result in the loss of its full or partial disability, destruction, distortion or leakage of information resulting from failures, accidental failures or the result of an intruder's unauthorized access Access to network resources. Early detection of such conditions will eliminate their cause in a timely manner, as well as prevent possible negative consequences. Therefore, to improve the reliability of the web resource, it is expedient to improve the identification methods. In order to solve this issue, a method was proposed and an algorithm for identification of threats of unauthorized access was developed and testing of the developed algorithm was presented. The obtained results allow to confirm the high accuracy of detection of abnormal network activity.

Відомості про авторів

Кец Дмитро Олександрович

Освіта: Повна вища, «Захист інформації в комп'ютерних системах та мережах» (2010).

Місце роботи: Вінницький національний технічний університет, Центр інформаційних технологій та захисту інформації.

Область знань: Захист програмного забезпечення, захист комп'ютерних мереж, криптографічний захист інформації.

Наукові інтереси: Захист мережевих ресурсів від несанкціонованого втручання, криптографічний захист інформації.

Email: *dima.kec@gmail.com*

Присяжний Дмитро Петрович

Освіта: Повна вища, «Програмне забезпечення автоматизованих систем» (2010).

Місце роботи: Вінницький національний технічний університет, Центр інформаційних технологій та захисту інформації.

Область знань: технології програмування, бази даних і знань, захист операційних систем.

Наукові інтереси: Захист баз даних, захист web-ресурсів.

E-mail: *dimpris@gmail.com*

Салієва Ольга Володимирівна

Освіта: Повна вища, «Педагогіка і методика середньої освіти. Математика і фізика» (2004).

Місце роботи: Вінницький національний технічний університет, Центр інформаційних технологій та захисту інформації.

Область знань: Математика, криптографія, безпека інформаційних систем.

Наукові інтереси: Теорія чисел, криптографічний захист інформації, безпека інформаційних систем.

E-mail: *salieva8257@gmail.com*

3. Забезпечення безпеки інформації в інформаційних системах

УДК 621. 3.06

БЛОЧНЫЙ ШИФР С УЛУЧШЕННЫМИ ПОКАЗАТЕЛЯМИ ПРИХОДА К СЛУЧАЙНОЙ ПОДСТАНОВКЕ

Лисицкий Константин
Харьковский национальный университет имени В. Н. Каразина

BLOCK CIPHER WITH IMPROVED PARAMETERS OF ARRIVAL TO RANDOM SUBSTITUTION

Lisitcky Konstantin
Kharkov national University name V.N. Karazin

Анотація: **На прикладі вдосконаленого шифру Калина-2 пропонуються конструкції SPN шифрів з поліпшеними показниками їх переходу до стану випадкової підстановки. Удосконалення ґрунтується на застосуванні першого циклового перетворення нової конструкції, що дозволяє активізувати всі S-блоки другого циклу. Шифри не поступаються за швидкодією відомим конструкціям і дозволяють без зменшення стійкості застосовувати в них випадкові S-блоки.**
Ключові слова: **SPN шифр, динамічні показники переходу шифру до стану випадкової підстановки, активні S-блоки, випадкові S-блоки, показники швидкодії.**
Summary: **Using the example of the improved Kalina-2 cipher, SPN cipher designs is proposed with improved indicators of their arrival to the state of random substitution. The improvement is based on the application of the first cyclic transformation of the new design, which allows activating all S-blocks of the second cycle. The ciphers are not inferior in speed to known designs and allow using random S-blocks without any reduction in their resistance.**
Keywords: **SPN cipher, dynamic cipher arrival rates to the random substitution state, active S-blocks, random S-blocks, performance indicators.**

Введение

Основным недостатком известных конструкций SPN блочных симметричных шифров является крайне малое число S-блоков, активизируемых разностями входных блоков данных. Мы снова возвращаемся к идее усовершенствования имеющихся конструкций блочных симметричных шифров (БСШ), которой посвящена работа [1]. В этой работе авторы пошли по пути введения на входе шифра дополнительного смешивающего преобразования на основе сложения по модулю 2 сегментов блоков данных на входе шифра полагая, что это позволит увеличить число активизируемых S-блоков первого цикла. Но как выяснилось в процессе исследований, этот подход оказался ошибочным. Он позволил увеличить число активизируемых S-блоков при активизации шифра однобайтовой разностью, но не исключил возможности активизации одного S-блока первого цикла в случае нескольких ненулевых разностей входного блока данных, например, в случае, когда для четвёрки сегментов входа $\Delta X_1 = 0$, $\Delta X_2 = \Delta X_3 = \Delta X_4 = \Delta \neq 0$. Это значит, что приведенные в [1] “усовершенствования” являются лишними и они не работают. Действительно, на входе шифра должны состояться асе возможные варианты входных блоков данных.

Оказалось справедливым утверждение того, что для SPN шифров с цикловыми функциями, использующими однослойные подстановочные преобразования

минимальное число активизируемых S-блоков первого цикла равно одному. Именно из-за этого процесс прихода БСШ к состоянию случайной подстановки затягивается до трёх и более циклов.

Следует, что единственная возможность увеличить число активизируемых S-блоков первого цикла – это сделать его двухслойным, как это сделано в шифрах Мухомор, IDEA NXT, ШУП-2 [2].

В этой работе показано, что двухслойное преобразование, рассмотренное, например, в шифре ШУП-2 [2], близко повторяет двухцикловую конструкцию. Его достоинством можно считать то, что оно позволяет обосновать возможность уменьшения числа циклов прихода шифра к состоянию случайной подстановки. Вторым его достоинством является возможность активизации всех S-блоков второго слоя преобразований первого цикла, которая затем распространяется и на остальные циклы. Этот эффект активизации S-блоков второго и последующих циклов может быть реализован и без второго слоя преобразований, т.е. при построении первого цикла по однослойной схеме, как это сделано в шифре ШУП-1 [2]. В этом случае необходимо позаботиться только о том, чтобы колонки матрицы состояний после сложения по модулю 2 выхода последнего SL преобразования первого слоя с выходами других SL преобразований были различными (не совпадали). Этого можно добиться, если для колонок на выходах преобразований первого слоя применить новую операцию, которой нет в оригинальном шифре. Эта операция заключается в циклическом сдвиге колонок матрицы состояний. Назовём её операцией ShiftColumns. Поскольку для 256 битного шифра получается 4 колонки матрицы состояний, то нужно сделать так, чтобы циклические сдвиги между колонками были различными.

1. Сущность предложения

Схема предлагаемой новой конструкции первого цикла для 256-ти битного шифра Калина представлена на Рис. 1. В этом случае на вход нового первого цикла поступает входной блок данных, преобразованный в матрицу состояний из четырёх колонок и восьми строк (восемь S-блоков в колонке) после его сложения с ключом забеливания, а SL преобразования берутся восьми байтовыми с умножением на МДР матрицы размером 8×8 (как в шифре Калина). Сложение с цикловым подключом для нового цикла (операция AddRoundKey) выполняется по модулю 2. После первого цикла используются стандартные преобразования шифра Калина.

Сам новый первый цикл вставляется в оригинальную конструкцию после первоначального забеливании вместо первого цикла оригинальной разработки.

Представленная конструкция содержит основные элементы схемы из работы [2], только в данном случае число SL преобразований в слое уменьшено до 4-х, так как в шифре Калина обрабатываются 64-х битные сегменты входного блока данных. Кроме того, в неё добавлено новое преобразование ShiftColumns и добавлено сложение с цикловым подключом (операция AddRoundKey). В этом случае SL преобразования являются, как уже отмечено выше, 8-ми байтовыми и содержат 8 параллельно включенных S-блоков, над выходами которых выполняется операция умножение на МДР матрицы размером 8×8 (это фактически преобразования SubBute и MixColumn шифра Калина). Преобразования SL включены в цепочку на вход текущего преобразования поступает выход предыдущего

В этом случае на вход нового первого цикла поступает входной блок данных, преобразованный в матрицу состояний из четырёх колонок и восьми строк (восемь S-блоков в колонке) после его сложения с ключом забеливания. Далее идут SL преобразования, которые включены в цепочку так, что на вход текущего SL преобразования совместно с текущим сегментом данных поступает выход предыдущего SL преобразования. После сложения последнего SL преобразования

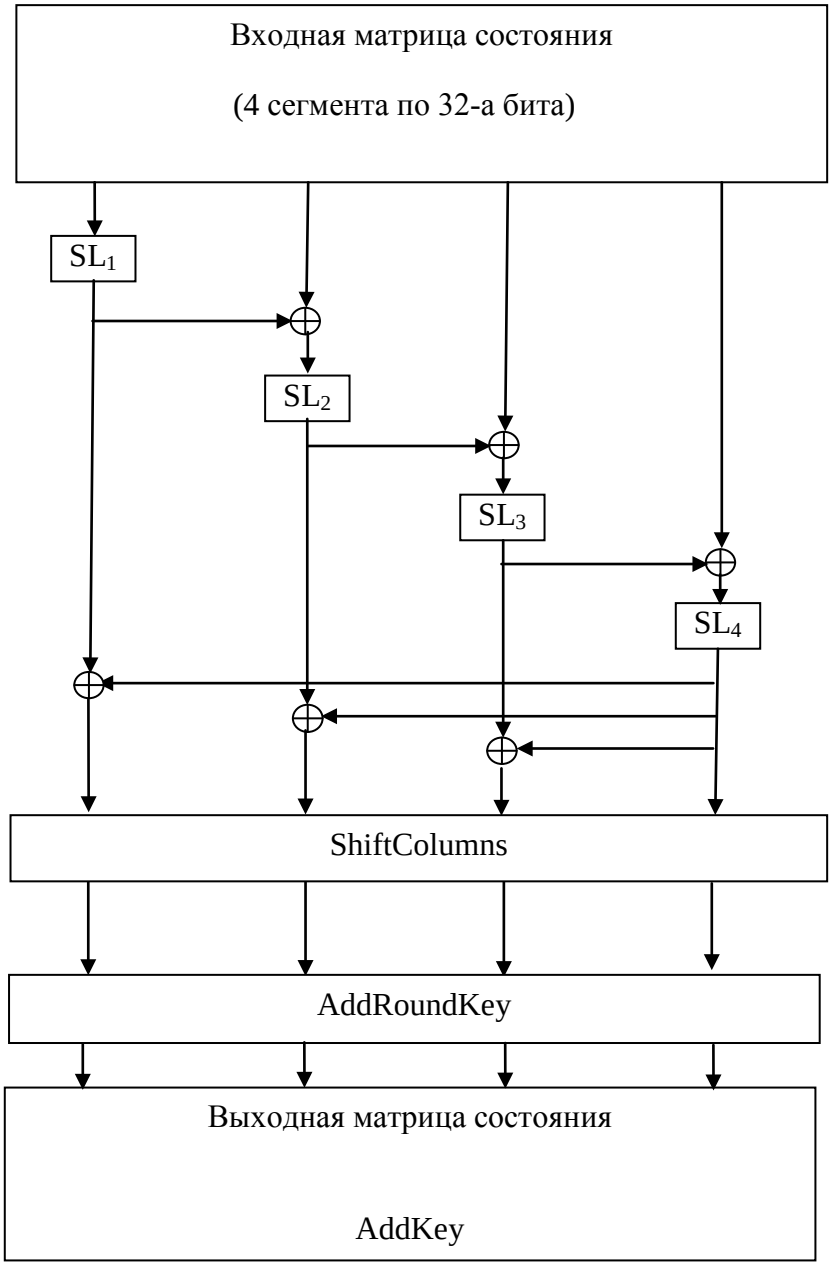


Рис. 1 – Схема усовершенствованного первого цикла шифра Калина

первого слоя с выходами других SL преобразований выполняется операция ShiftColumns и цикл завершается сложением полученного результата с цикловым подключом по модулю 2.

После первого цикла идут стандартные преобразования шифра Калина

2. Показатели случайности

Оценим показатели случайности такого двухциклового преобразования. При однобайтовой разности входного блока данных для самого правого SL преобразования первого слоя в худшем случае активизируется один из S-блоков этого SL преобразования, который после МДР преобразования активизирует все 8 байтов 4-ой колонки матрицы состояний. Эта колонка после сложения с выходами всех предыдущих SL преобразований формирует все четыре колонки матрицы состояний из активных байтов. Последующее преобразование ShiftColumns осуществляет перестановку байтов в каждой из колонок, которые поступают на входы всех SL преобразований второго цикла и активизируют все 32 его S-блока. Возможные варианты прохождения МДР преобразования иллюстрирует Таблица 1, заимствованная из работы [3].

Таблица 1.

Двоичный логарифм вероятности перехода вектора активизации через 8-ми байтный MixColumns

Вх. \ Вых.	0	1	2	3	4	5	6	7	8
0	0	-	-	-	-	-	-	-	-
1	-	-	-	-	-	-	-	-	–0,046
2	-	-	-	-	-	-	-	–7,99	–0,045
3	-	-	-	-	-	-	15,9	–8,04	–0,045
4	-	-	-	-	-	–23,9	–16,0	–8,04	–0,045
5	-	-	-	-	–31,9	–24,0	–16,0	–8,04	–0,045
6	-	-	-	–39,9	–32,0	–24,0	–16,0	–8,04	–0,045
7	-	-	–47,9	–40,0	–32,0	–24,0	–16,0	–8,04	–0,045
8	-	–55,9	–48,0	–40,0	–32,0	–24,0	–16,0	–8,04	–0,045

8 ненулевых разностей на входе МДР преобразования активизируют

– один S-блок следующего цикла (колонку матрицы состояний) с вероятностью 2^{56}. Вероятность прохода SL преобразования второго цикла

$$2^{-56}\times 2^{-6} = 2^{-62};$$

– два S-блока следующего цикла (колонку матрицы состояний) с вероятностью 2^{-48}. Вероятность прохода SL преобразования второго цикла

$$2^{-48}\times (2^{-6})^2 = 2^{-60};$$

– три S-блока следующего цикла (колонку матрицы состояний) с вероятностью 2^{-40}. Вероятность прохода SL преобразования второго цикла

$$2^{-40}\times (2^{-6})^3 = 2^{-68};$$

– четыре S-блока следующего цикла (колонку матрицы состояний) с вероятностью 2^{-32}. Вероятность прохода SL преобразования второго цикла

$$2^{-32}\times (2^{-6})^4 = 2^{-56};$$

– пять S-блоков следующего цикла (колонку матрицы состояний) с вероятностью 2^{-24}. Вероятность прохода SL преобразования второго цикла

$$2^{-24}\times (2^{-6})^5 = 2^{-54};$$

– шесть S-блоков следующего цикла (колонку матрицы состояний) с вероятностью 2^{-16}. Вероятность прохода SL преобразования с второго цикла

$$2^{-16}\times (2^{-6})^6 = 2^{-52};$$

– семь S-блоков следующего цикла (колонку матрицы состояний) с вероятностью 2^{-8}. Вероятность прохода SL преобразования следующего цикла

$$2^{-8}\times (2^{-6})^7 = 2^{-50};$$

– восемь S-блоков следующего цикла (колонку матрицы состояний) с вероятностью $2^{-0,045}$. Вероятность прохода SL преобразования второго цикла

$$(2^{-6})^8 = 2^{-48}.$$

Из этого следует, что вариант с прохождением через SL преобразование 8 S-блоков является наиболее вероятным.

Для 4 SL преобразований в последнем случае имеем вероятность прохождения через SL преобразования второго цикла равную $(2^{-48})^4 = 2^{-106}$. С учётом первого цикла имеем $(2^{-6})^{32}\times 2^{-106} = 2^{-324} >> 2^{-250}$.

Все другие ситуации будут менее вероятными (они не будут ухудшать оценки).

Здесь расчёт выполнен для дифференциальных и линейных показателей S-блоков шифра Rijndael с $DP^{\pi}_{\max} = LP^{\pi}_{\max} = 2^{-6}$.

Очевиден большой запас по стойкости. Далее можно воспользоваться результатами работы [1], из которых следует, что рассмотренная конструкция шифра позволяет без потери стойкости применять случайные S-блоки.

Заметим, что оригинальная версия шифра Калина приходит к случайной подстановке за 4 цикла, а предложенная конструкция приходит к состоянию случайной подстановки за три цикла. При этом за три

цикла активизируется 65 S-блоков, в то время как в Калине за три цикла активизируется 41 S-блок.

4. Показатели вычислительной сложности

Как и в работе [4] при оценке вычислительной сложности мы будем ориентироваться на число XOR операций, выполняемых шифром в процессе зашифрования и расшифрования. Исходим из того, что для выполнения SL преобразования (матричного умножения) требуется выполнить три XOR операции.

Тогда в соответствии со структурой циклового преобразования, представленной на Рис. 1, в новом первом цикле потребуется выполнить 4 + 4×7 = 32 XOR операций (такта). Для 8-ми циклового шифра потребуется выполнить 32 + 32×7 = 224-е XOR операций.

В Калине-256 на 14 циклов приходится 32×14 = 448 XOR операций, т. е. усовершенствованная Калина будет вдвое быстрее оригинальной разработки.

При этом ещё не учитываются затраты на процедуру разворачивания мастер-ключа.

Выводы

В работе предложена конструкция усовершенствованного шифра Калина с улучшенными показателями прихода шифра к состоянию случайной подстановки. Основой построения шифра является применение при построении первого цикла слоя преобразований с управляемыми друг другом подстановками. Предложенное усовершенствование реализует возможность активизации всех S-блоков второго цикла. Усовершенствованный шифр позволяет уменьшить допустимое число циклов шифрования, что приводит к повышению его производительности по сравнению с оригинальной версией без снижения стойкости.

В предложенном шифре могут применяться случайные S-блоки без специального отбора, что открывает реальный путь устранения зависимости свойств шифра от свойств применяемых в шифрах S-блоков.

Перелік посилань

[1] В. И. Долгов, *Усовершенствованный блочный симметричный шифр Калина* / В. И. Долгов, И. В. Лисицкая, К. Е. Лисицкий // 0485-8972. – Радиотехника: Всеукр. межвед. научн.-техн. сб. – 2016. – Вып.186. – С. 119-131.

[2] В. И. Долгов, *Новая концепция проектирования блочных симметричных шифров* / В. И. Долгов, И. В. Лисицкая, К. Е. Лисицкий // 0485-8972.– Радиотехника: Всеукр. межвед. научн.-техн. сб. – 2016. – Вып.186. – С. 132-152.

[3] В. И. Руженцев, *О методе доказательства стойкости блочных шифров к атаке невыполнимых дифференциалов* / В. И. Руженцев // Applied radio electronics, Scientific and Technical Journal. – 2013 – Vol. 12, № 2. – С. 215-219.

[4] И. Д. Горбенко, *Свойства и возможности оптимизации криптографических преобразований в AES – RIJNDAEL* / И. Д. Горбенко, Д. А. Чекалин // Радиотехника. Всеукр. Межвед. Науч.-техн. сб. 2001. Вып. 119. С. 36-42.

References

[1] V. I. Dolgov, *Usovershenstvovanyj blochnyj simmetrichny shifr Kalina* / V. I. Dolgov, I. V. Lisitskaya, K. E. Lisitsky // 0485-8972. – Radiotehnika. – Vseukr. Mezhved. Naych.- tehn. zb – 2016. – Vyp. 186. – P. 119-131.

[2] V. I. Dolgov, *Novaya Koncepciya proektirovaniya blochnyh simmetrichnyh shifrov* / V. I. Dolgov, I. V. Lisitskaya, K. E. Lisitsky // 0485-8972 Radiotehnika – Vseukr. Mezhved. Naych.- tehn. zb – 2016. – Vyp. 186. – P. 132-152.

[3] V. I. Ruzhencev, *O metode dokazatelstva stojkosti blochnyh shifrov k atake nevypolnimyh differencialov* / V. I. Ruzhencev // Applied radio electronics, Scientific and Technical Journal. – 2013 – Vol. 12, № 2. – S. 215-219.

[4] I. D. Gorbenko, *Svojstva i vozmozhnosti optimtzacii kriptjgraficheskih preobrazovanij v AES* / I. D. Gorbenko, D. A. Chekalin // Vseukr. Mezhved. Naych.- tehn. zb – 2001. Vyp. 119.– P. 36-42.

Реферат

Лисицький Костянтин

Блоковий шифр з поліпшеними показниками приходу до випадкової підстановки

Основним недоліком відомих конструкцій SPN блокових симетричних шифрів є вкрай мале мінімальне число S-блоків, що активізуються однобайтовими різницями

вхідних блоків даних. Спроби збільшення числа активізуємих S-блоків на перших циклах шифрування шифру Калина на основі введення на вході шифру додаткового змішуючого перетворення шляхом додавання за модулем 2 сегментів даних на вході шифру не дає очікуваного ефекту. Для цього на вході шифру повинні відбутися всі можливі варіанти вхідних блоків даних.

Сутність запропонованого нового удосконалення, яке будується на основі ведення в 256-ти бітний шифр Калина після операції забілювання на його вході замість першого циклу нового циклового перетворення. Це перетворення включає в себе шар послідовно включених в ланцюжок чотирьох SL перетворень, які представляють собою паралельне включення восьми байтових S-блоків (операція ByteSub в Калині) з наступним множенням значень виходів S-блоків на МДВ матрицю розміру 8×8 (операція MixColumn в Калині). При цьому поточне SL перетворення приймає на вхід суму за модулем 2 разом з черговим вхідним сегментом даних (колонкою) результат попереднього SL перетворення. Значення виходу останнього SL перетворення в ланцюжку використовують для формування останньої колонки нової матриці стану, а виходи попередніх SL перетворень після їх підсумовування за модулем 2 з виходом останнього SL перетворення використовують для формування інших колонок матриці стану. На завершення колонки нової матриці стану піддають циклічному зсуву вгору на певну (різну) кількість байтів (операція ShiftColumn), складають їх за модулем 2 з цикловим підключем (операція XORRoundKey) і подають на вихід нового циклу, причому загальне число циклів шифру зменшують до восьми .

При однобайтовій різниці вхідного блоку даних (колонки) для самого правого SL перетворення першого шару в гіршому випадку активізується один з S-блоків цього SL перетворення, який після МДВ перетворення активізує всі 8-м байтів на його виході (колонки матриці стану). Подальше перетворення ShiftColumns здійснює перестановку байтів в кожній з колонок, які надходять на входи всіх SL перетворень другого циклу і активізують практично всі 32-а його S-блоку, тобто забезпечується активізація всіх S-блоків другого і наступних циклів.

Шифр з удосконаленням перевищує за швидкодією вихідну конструкцію і дозволяє без зменшення стійкості застосовувати в шифрі випадкові S-блоки.

Лисицкий Константин

Блочный шифр с улучшенными показателями прихода к случайной подстановки

Основным недостатком известных конструкций SPN блочных симметричных шифров является крайне малое минимальное число S-блоков, активизируемых однобайтовыми разностями входных блоков данных. Работы, посвященной разработке предложения по увеличения числа S-блоков активизируемых на первых циклах зашифрования шифра Калина на основе введения на входе шифра дополнительного смешивающего преобразования путём сложения по модулю 2 сегментов данных на входе шифра не даёт ожидаемого эффекта. Длят этого на входе шифра должны состояться все возможные варианты входных блоков данных.

Сущность предлагаемого усовершенствования, строится на основе ведения в 256-ти битный шифр Калина после операции забеливания на его входе вместо первого цикла нового циклового преобразования. Это преобразование включает в себя слой последовательно включенных в цепочку четырех SL преобразований, которые представляют собой параллельное включение восьми байтовых S-блоков (операция ByteSub в Калине) с последующим умножением значений выходов S-блоков на МДР матрицу размера 8×8 (операция MixColumn в Калине). При этом текущее SL преобразования принимает на вход сумму по модулю 2 вместе с очередным входным сегментом данных (колонкой) результат предыдущего SL преобразования. Значение выхода последнего SL преобразования в цепочке используют для формирования последней колонки новой матрицы состояния, а выходы предыдущих

SL преобразований после их суммирования по модулю 2 с выходом последнего SL преобразования используют для формирования других колонок матрицы состояния. В завершение колонки получившейся новой матрицы состояния подвергают циклическому сдвигу вверх на определенное (различное) количество байтов (операция ShiftColumn), складывают их по модулю 2 с цикловым подключем (операция XORRoundKey) и подают на выход нового цикла, причем общее число циклов шифра уменьшают до восьми.

При однобайтовой разности входного блока данных (колонки) для самого правого SL преобразования первого слоя в худшем случае активизируется один из S-блоков этого SL преобразования, который после МДР преобразования активизирует все 8-мь байтов на его выходе (колонку матрицы состояния). Последующее преобразование ShiftColumns осуществляет перестановку байтов в каждой из колонок, которые поступают на входы всех SL преобразований второго цикла и активизируют практически все 32-а его S-блока, т.е. обеспечивается активизация всех S-блоков второго и последующих циклов.

Шифр с усовершенствованием превышает по быстродействию исходную конструкцию и позволяет без уменьшения стойкости применять в шифре случайные S-блоки.

Lisicky Konstantin

Block cipher with improved parameters of arrival to random substitution

The main drawback of the known SPN designs of block symmetric ciphers is the extremely small minimum number of S-blocks activated by single-byte differences in the input data blocks. Try to increase the number of S-boxes activated on the first encryption cycles of the Kalina cipher. It is building based on introducing an additional mixing transformation at the input of the cipher by adding modulo 2 data segments at the input of the cipher does not give the expected effect. Indeed, at the input of the cipher, all possible input data block variants should take place.

The essence of the proposed new improvement, which is basing on reference to the 256-bit cipher of Kalina after the operation of whitening at its entrance instead of the first cycle of a new cyclic transformation. This transformation includes a layer of consecutively included in the chain of four SL transforms, which are the parallel inclusion of the eight byte S-boxes (ByteSub operation in Kalina), followed by multiplying the values of the

S-block outputs by the MDR 8×8 matrix (MixColumn operation in Kalina). While the current

SL transform takes an input modulo 2 together with the next input data segment (column) the result of the previous SL transformation. Next, the output value of the last SL transformation in the chain is used to form the last column of the new state matrix, and the outputs of the previous

SL transforms after their summation modulo 2 with the output of the last SL conversion are used to form other columns of the state matrix. Finally, the columns of the resulting new state matrix are cycled up to a certain (different) number of bytes (the ShiftColumn operation), stacking them modulo 2 with a cyclic connection (operation XORRoundKey), and outputting a new cycle, the total number of cipher cycles being reduced to eight.

For a single-byte difference in the input data block (column) for the rightmost SL conversion of the first layer, in the worst case, one of the S-blocks of this SL transformation is activated, which after the MDS conversion activates all 8-bytes at its output. Subsequent transformation of ShiftColumns performs rearrangement of bytes in each of the columns, which enter the inputs of all SL transforms of the second cycle and activate practically all 32 of its S-blocks, i.e. All S blocks of the second and subsequent cycles are activated.

The ciphers are not inferior in speed to known designs and allow us, without reducing the durability, to use in the cipher random S-blocks.

Відомості про авторів

Лисицький Костянтин Євгенійович

Освіта: аспірант кафедри БІСТ Харківського національного університету імені В.Н. Каразіна.

Наукові інтереси: Криптографія, криптоаналіз, технології блочного симетричного шифрування.

Email: *lisitskaiv@ukr.net*

УДК 638.235.231

УТОЧНЕНИЕ ПОРОГОВОГО ЗНАЧЕНИЯ ПРИ КЛАССИФИКАЦИИ БЛОКОВ ЦИФРОВОГО ИЗОБРАЖЕНИЯ ДЛЯ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ ВЫЯВЛЕНИЯ ФОТОМОНТАЖА

Мокрицкий Вадим; Зорило Виктория; Ворникова Мария; Креминский Владислав; Лычов Роман; Матвеева Анастасия; Мурова Вероника; Шпортюк Анастасия
Одесский национальный политехнический университет

UPDATE OF THRESHOLD VALUE AT CLASSIFICATION OF DIGITAL IMAGE BLOCKS FOR IMPROVING EFFICIENCY OF DETECTING PHOTOMONTAIS

Mokritsky Vadym; Zorilo Viktoriya; Vornikova Maria; Kreminsky Vladislav; Lychov Roman; Matveeva Anastasia; Murova Veronika; Shportyuk Anastasia
Odessa National Polytechnic University

Анотація: **Задачі класифікації блоків зображень часто виникають в галузі захисту цифрових зображень від можливих порушень цілісності, а також в галузі розпізнавання образів. У даній роботі проведено аналіз блоків зображень на предмет уточнення порогового значення при їх класифікації способом, запропонованим раніше, який засновано на аналізі функції їх яскравості. Встановлено розміри блоків, а також порогове значення, при яких досягнуто кращої точності виділення контурів цифрового зображення.**
Ключові слова: **Виділення контурів, цифрове зображення, класифікація блоків зображення, функція яскравості, інформаційна безпека.**
Summary: **The tasks of classifying image blocks often arise in the field of protecting digital images from possible integrity violations, as well as in pattern recognition. In this paper, an analysis of image blocks is performed to refine the threshold value when they are classified by the method proposed earlier, based on the analysis of their brightness function. The sizes of the blocks are set, as well as the threshold value at which the best accuracy of the outlines of the digital image contours is achieved.**
Keywords: **Contour selection, digital image, block classification, brightness function, information security.**

Введение

Решение задачи выделения текстурных признаков цифрового изображения актуально во многих областях: компьютерная диагностика, анализ снимков со спутника, системы видеонаблюдения в охране, системы навигации и т.д. В настоящий момент понятие текстуры цифрового изображения (ЦИ) интерпретируют по-разному в зависимости от конкретных задач обработки изображений, а качество их проверяется эмпирически для каждой задачи классификации. Поэтому синтез большого количества текстурных признаков и исследования их на информативность является актуальным [1]. В [2] текстуру определяют как пространственную организацию элементов в пределах некоторого участка поверхности, которая обусловлена определенным статистическим распределением интенсивности серых тонов или тонов различного цвета. Участок считают текстурным, если количество отмечаемых на нем перепадов интенсивности или изменений цвета достаточно велико. В [3] текстура определяется как некоторым образом организованный участок поверхности. В [4] под текстурой понимают матрицу или фрагмент пространственных свойств участков изображений с однородными статистическими характеристиками. Важными понятиями текстуры являются

фон и контур. В работе [5] под текстурой изображения понимаются фон и контур. Предложен способ классификации блоков матрицы изображения, основанный на анализе функции их яркости, в соответствии с которым выделены четыре категории блоков: фоновые и три категории контурных (с сильно-выраженным, средне-выраженным и слабо выраженным контуром). Приведенная классификация выполнена для блоков размером 8×8 и позволяет с определенной точностью выделять контуры объектов на изображении. Блок относят к той или иной категории, сравнивая разность максимального и минимального значений яркости пикселей с пороговым значением, рекомендации относительно которого были получены эмпирически. Необходимость в подобной классификации возникла в связи с решением вопросов выявления фотомонтажа. Эффективность некоторых методов, в частности метода, описанного в [6], зависит от частотной составляющей сигнала изображения. При низком уровне высокочастотной составляющей (часть изображения без контуров или со слабо выраженными контурами) этот метод справляется с задачей, а в противном случае его использование не целесообразно. Данный факт указывает на возможность применения описанного в [5] способа классификации блоков изображения в области информационной безопасности. Также в работе даны рекомендации относительно уточнения границ выделенных объектов, используя при этом блоки меньших размеров. Однако при изменении размера блока необходимо также учитывать и необходимость коррекции порогового значения.

Цель данной работы – повысить точность выделения границ объектов на изображении способом, основанном на анализе функции яркости блоков цифрового изображения.

Для достижения данной цели необходимо решить следующие задачи: определить размеры блока, при которых будет достигнут наилучший результат; уточнить пороговое значение для наилучшего выделения контуров изображения.

Материалы и методы

Пусть R,G,B – $n\times n$-матрицы красного, зеленого и синего спектров блока

ЦИ соответственно. Согласно [5] блок относится к классу F (фоновый), если для каждой из матриц R,G,B выполняется условие

$$\max\left(a_{ij}-b_{ij}\right)\le 30, \qquad (1)$$

и к классу K (контурный) в противном случае, a_{ij} и b_{ij} – элементы матриц R,G,B, $a_{ij}\ne b_{ij}$, $1\le i\le n$, $1\le j\le n$.

Блоки класса K в свою очередь были разделены на категории $K1$, $K2$ и $K3$: со слабой, средней и высокой четкостью контуров соответственно. Категории $K1$ принадлежат такие блоки, для которых по одной из трех матриц R,G,B выполняется условие

$$\max\left(a_{ij}-b_{ij}\right)>30, \qquad (2)$$

a_{ij} и b_{ij} – элементы матриц R,G,B, $a_{ij}\ne b_{ij}$, $1\le i\le n$, $1\le j\le n$.

Для блоков категории $K2$ условие (2) должно выполняться для любых двух из трех матриц R,G,B. В блоках категории $K3$ условие (2) должно выполняться для каждой из матриц R,G,B. Алгоритм классификации блоков матрицы ЦИ состоит из следующих шагов:

1. Для матриц R,G,B блока ЦИ найти максимальный и минимальный элементы, определить разницу между ними.
2. Провести классификацию блока.

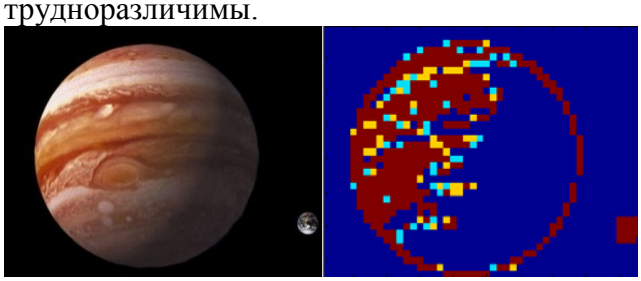
2.1. Если для каждой из матриц R,G,B выполняется условие (1), то блок принадлежит классу F.

2.2. Если для одной из матриц R,G,B блока не выполняется условие (1), то блок принадлежит категории $K1$ класса K.

2.3. Если для любых двух матриц R, G, B блока не выполняется условие (1), то блок принадлежит категории $K2$ класса K.

2.4. Если для каждой из матриц R, G, B блока выполняется условие (2), то блок принадлежит категории $K3$ класса K.

На рис. 1 выполнена классификация для блоков размером 8×8. Выделение контуров происходит грубо – детали трудноразличимы.

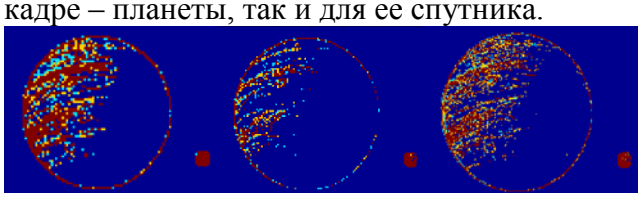


а б

Рис. 1 – а) ЦИ; б) категории блоков (синий, голубой, желтый, крсный – F, $K1, K2, K3$ соответственно)

Для эксперимента использовали 100 изображений из базы NRSC [7] как в форматах с потерями, так и без потерь. Матрицы изображений разбивали на блоки 4×4, 3×3, 2×2 (рис. 2, а, б, в). Эксперимент был проведен при использовании среды Matlab.

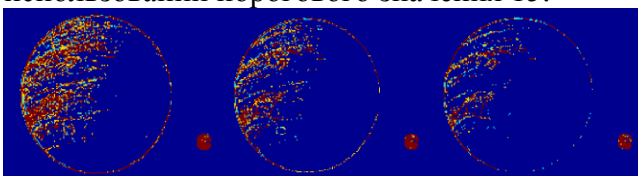
Результаты и их обсуждение. Рассмотрим, что происходит при уменьшении размера блоков. На рисунке 2 можем видеть, что при уменьшении размера блоков выделение мелких деталей, как и выделение очертаний объектов в целом, происходит более эффективно, чем в первоначальном варианте. Это наблюдается как для большого объекта в кадре – планеты, так и для ее спутника.



а б в

Рис. 2 – Выбор размера блока: а – 4×4; б – 3×3, в – 2×2

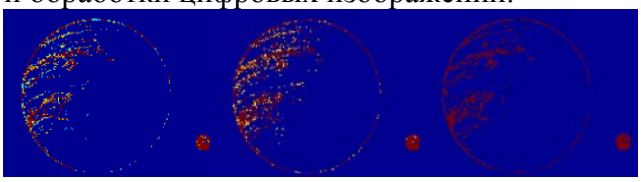
Выбор порогового значения (рис. 3, а, б, в) осуществляли путем субъективного ранжирования с привлечением экспертной группы из 10 человек. При анализе ста изображений установлено, что для блоков 2×2 наилучшие результаты получены при использовании порогового значения 15.



а б в

Рис. 3 – Выбор порогового значения: а – 10; б – 15, в – 20

На рисунке 4 продемонстрированы варианты выделения контуров различных категорий и это может найти свое применение в области защиты информации и обработки цифровых изображений.



а б в

Рис. 4 – Выделение контуров разных категорий: а – Все три категории; б – $K2$ и $K3$; в – $K3$

Выводы

Таким образом, по результатам работы удалось повысить точность выделения контуров способом, предложенным ранее в [5]. Получены рекомендации относительно выбора размера блоков и порогового значения. Путем субъективного ранжирования установлено, что при пороговом значении 15 для блоков размером 2×2 точность выделения контуров существенно повышается, Поставленные в работе задачи решены, цель достигнута.

Перелік посилань

[1] Н. В. Клодникова, *Обзор текстурных признаков для задач распознавания образов*/ Н. В. Клодникова // Доклады ТУСУРа. 2004 г. Автоматизированные системы обработки информации, управления и проектирования – 2004. – С. 113-124.

[2] Г. А. Андреев, *Анализ и синтез случайных пространственных текстур* / Г. А. Андреев, О. В. Базарский, А. С. Глауберман, А. И. Колесников, Ю. В.Коржик, Я. Л. Хлявич // Зарубежная радиоэлектроника. – 1984. – №2. – С. 3–33.

[3] Р. М. Харалик, *Статистический и структурный подходы к описанию текстур* // ТИИЭР. – 1979. – Т. 67. – № 5.

[4] А. А. Потапов, *Новые информационные технологии на основе вероятностных текстурных и фрактальных признаков в радиолокационном обнаружении малоконтрастных целей* // Радиотехника и электроника. – 2003. – Т. 48. – № 9. – С. 1101–1119.

[5] В. В. Зорило, *Способ классификации блоков матрицы цифрового изображения* / В. В. Зорило // Інформатика та математичні методи в моделюванні. – 2012. – №4, Т.2. – С. 168-174.

[6] А. А. Кобозєва, *Метод виявлення фальсифікації цифрового зображення в умовах збурних дій* / А. А. Кобозєва, В. В. Зоріло // Збірник наукових праць військового інституту національного університету імені Тараса Шевченка. – 2009. – № 20. – С.147-153.

[7] NRCS Photo Gallery: *[Электронный ресурс]* // United States Department of Agriculture. Washington, USA. Режим доступа: http://photogallery.nrcs.usda.gov (Дата обращения: 26.04.2017).

References

[1] N. V. Klodnykova, *Obzor teksturnыkh pryznakov dlia zadach raspoznavanyia obrazov*/ N. V. Klodnykova // Dokladы TUSURa. 2004 h. Avtomatyzyrovannыe systemы obrabotky ynformatsyy, upravlenyia y proektyrovanyia – 2004. – S. 113-124.

[2] H. A. Andreev, *Analyz y syntez sluchainыkh prostranstvennыkh tekstur* / H. A. Andreev, O. V. Bazarskyi, A. S. Hlauberman, A. Y. Kolesnykov, Yu. V.Korzhyk, Ya. L. Khliavych // Zarubezhnaia radyoэlektronyka. – 1984. – #2. – S. 3–33.

[3] R. M. Kharalyk, *Statystycheskyi y strukturnыi podkhodы k opysanyiu tekstur* // TYYЭR. – 1979. – T. 67. – # 5.

[4] A. A. Potapov, *Novыe ynformatsyonnыe tekhnolohyy na osnove veroiatnostnыkh teksturnыkh y fraktalnыkh pryznakov v radyolokatsyonnom obnaruzhenyy malokontrastnыkh tselei* // Radyotekhnyka y эlektronyka. – 2003. – T. 48. – # 9. – S. 1101–1119.

[5] V. V. Zorylo, *Sposob klassyfykatsyy blokov matrytsы tsyfrovoho yzobrazhenyia* / V. V. Zorylo // Informatyka ta matematychni metody v modeliuvanni. – 2012. – #4, T.2. – S. 168-174.

[6] A. A. Kobozieva, *Metod vyiavlennia falsyfikatsii tsyfrovoho zobrazhennia v umovakh zburnykh dii* / A. A. Kobozieva, V. V. Zorilo // Zbirnyk naukovykh prats viiskovoho instytutu natsionalnoho universytetu imeni Tarasa Shevchenka. – 2009. – # 20. – S.147-153.

[7] NRCS Photo Gallery: [Эlektronnыi resurs] // United States Department of Agriculture. Washington, USA. Rezhym dostupa: http://photogallery.nrcs.usda.gov (Data obrashchenyia: 26.04.2017).

Реферат

Мокрицький Вадим; Зоріло Вікторія; Ворнікова Марія; Кремінський Владислав; Личов Роман; Матвеєва Анастасія; Мурова Вероніка; Шпортюк Анастасія

Уточнення порогового значення при класифікації блоків цифрового зображення для підвищення ефективності виявлення фотомонтажу

Рішення завдання виділення текстурних ознак цифрового зображення актуально в багатьох областях: комп'ютерна діагностика, аналіз знімків з супутника, системи відеоспостереження, системи навігації і т.д. На даний момент поняття текстури цифрового зображення інтерпретують по-різному в залежності від конкретних завдань обробки зображень, а якість їх перевіряється емпірично для кожного завдання класифікації, тому синтез великої кількості текстурних ознак і дослідження їх на інформативність є актуальним. Важливими поняттями текстури є фон і контур. Раніше було запропоновано спосіб класифікації блоків матриці зображення, заснований на аналізі функції їх яскравості, відповідно до якого виділено чотири категорії блоків: фонові і три категорії контурних (з сильно-вираженим, середньо-вираженим і слабо вираженим контуром). Наведена класифікація виконана для блоків розміром

8 × 8 і дозволяє з певною точністю виділяти контури об'єктів на зображенні. Блок відносять до тієї чи іншої категорії, порівнюючи різницю максимального і мінімального значень яскравості пікселів з граничним значенням, рекомендації щодо якого були отримані емпірично. Необхідність у подібній класифікації виникла в зв'язку з вирішенням питань виявлення фотомонтажу. Ефективність деяких методів залежить від частотної складової сигналу зображення: при низькому рівні високочастотної складової (частина зображення без контурів або зі слабо вираженими контурами) метод справляється із завданням, а в іншому випадку його використання не доцільно. Даний факт вказує на можливість застосування способу класифікації блоків зображення в області інформаційної безпеки. Також в роботі надані рекомендації щодо уточнення меж виділених об'єктів, використовуючи при цьому блоки менших розмірів. Однак при зміні розміру блоку необхідно також враховувати і необхідність корекції порогового значення. Мета даної роботи - підвищити точність виділення меж об'єктів на зображенні способом, який заснований на аналізі функції яскравості блоків цифрового зображення.

В роботі показано, що при зменшенні розміру блоків виділення дрібних деталей, як і виділення контурів об'єктів в цілому, відбувається більш ефективно, ніж в початковому варіанті. Це спостерігається як для великого об'єкта в кадрі - планети, так і для її супутника.

Вибір порогового значення здійснювали шляхом суб'єктивного ранжирування. При аналізі ста зображень встановили, що для блоків 2 × 2 найкращі результати отримані при використанні порогового значення 15.

Таким чином, в результаты роботи вдалося підвищити точність виділення контурів способом, запропонованим раніше. Отримано рекомендації щодо вибору розміру блоків і порогового значення. Шляхом суб'єктивного ранжирування встановлено, що при пороговому значенні 15 для блоків розміром 2 × 2 точність виділення контурів істотно підвищується, Поставлені в роботі завдання вирішені, мета досягнута.

Мокрицкий Вадим; Зорило Виктория; Ворникова Мария; Креминский Владислав; Лычов Роман; Матвеева Анастасия; Мурова Вероника; Шпортюк Анастасия

Уточнение порогового значения при классификации блоков цифрового изображения для повышения эффективности выявления фотомонтажа

Решение задачи выделения текстурных признаков цифрового изображения актуально во многих областях: компьютерная диагностика, анализ снимков со спутника, системы видеонаблюдения, системы навигации и т.д. В настоящий момент понятие текстуры цифрового изображения интерпретируют по-разному в зависимости от конкретных задач обработки изображений, а качество их проверяется эмпирически для каждой задачи классификации, поэтому синтез большого количества текстурных признаков и исследования их на информативность является актуальным. Важными понятиями текстуры являются фон и контур. Ранее был предложен способ классификации блоков матрицы изображения, основанный на анализе функции их яркости, в соответствии с которым выделены четыре категории блоков: фоновые и три категории контурных (с сильно-выраженным, средне-выраженным и слабо выраженным контуром). Приведенная классификация выполнена для блоков размером 8×8 и позволяет с определенной точностью выделять контуры объектов на изображении. Блок относят к той или иной категории, сравнивая разность максимального и минимального значений яркости пикселей с пороговым значением, рекомендации относительно которого были получены эмпирически. Необходимость в

подобной классификации возникла в связи с решением вопросов выявления фотомонтажа. Эффективность некоторых методов зависит от частотной составляющей сигнала изображения: при низком уровне высокочастотной составляющей (часть изображения без контуров или со слабо выраженными контурами) метод справляется с задачей, в противном случае его использование не целесообразно. Данный факт указывает на возможность применения способа классификации блоков изображения в области информационной безопасности. Также в работе даны рекомендации относительно уточнения границ выделенных объектов, используя при этом блоки меньших размеров. Однако при изменении размера блока необходимо также учитывать и необходимость коррекции порогового значения. Цель данной работы – повысить точность выделения границ объектов на изображении способом, который основан на анализе функции яркости блоков цифрового изображения.

В работе показано, что при уменьшении размера блоков выделение мелких деталей, как и выделение очертаний объектов в целом, происходит более эффективно, чем в первоначальном варианте. Это наблюдается как для большого объекта в кадре – планеты, так и для ее спутника.

Выбор порогового значения осуществляли путем субъективного ранжирования. При анализе ста изображений установили, что для блоков 2×2 наилучшие результаты получены при использовании порогового значения 15.

Таким образом, в результате работы удалось повысить точность выделения контуров способом, предложенным ранее. Получены рекомендации относительно выбора размера блоков и порогового значения. Путем субъективного ранжирования установлено, что при пороговом значении 15 для блоков размером 2×2 точность выделения контуров существенно повышается, Поставленные в работе задачи решены, цель достигнута.

Mokritsky Vadym; Zorilo Viktoriya; Vornikova Maria; Kreminsky Vladislav; Lychov Roman; Matveeva Anastasia; Murova Veronika, Shportyuk Anastasia

Refinement of the threshold value in the classification of digital image blocks to improve the efficiency of detecting photomontage

The solution of the task of isolating the texture attributes of a digital image is relevant in many areas: computer diagnostics, analysis of satellite imagery, video surveillance systems, navigation systems, etc. At the moment, the concept of digital image texture (CI) is interpreted differently depending on the specific tasks of image processing, and their quality is tested empirically for each classification problem, so the synthesis of a large number of textural features and their research on information is relevant. Important concepts of the texture are the background and the outline. Previously, a method for classifying image matrix blocks based on an analysis of their brightness function was proposed, according to which four categories of blocks were identified: background and three categories of contour ones (with a strongly pronounced, medium-pronounced and weakly expressed contour). The above classification is made for blocks measuring 8 × 8 and allows you to accurately isolate the contours of objects in the image. A block is assigned to a category by comparing the difference between the maximum and minimum values of the pixel brightness with a threshold value, the recommendations for which were obtained empirically. The need for such a classification arose in connection with the solution of the issues of identifying photomontage. The effectiveness of some methods depends on the frequency

component of the image signal: at a low level of the high-frequency component (part of the image without contours or with poorly expressed contours), the method copes with the task, otherwise its use is not advisable. This fact indicates the possibility of applying the method of classifying image blocks in the area of information security. Also in the work recommendations are given regarding the specification of the boundaries of the selected objects, using blocks of smaller sizes. However, when changing the block size, it is also necessary to take into account the need to correct the threshold value. The purpose of this work is to improve the accuracy of the selection of the boundaries of objects in the image by a method based on the analysis of the brightness function of digital image blocks.

In the paper it is shown that when the size of blocks decreases, the allocation of small details, as well as the isolation of the outlines of objects as a whole, occurs more efficiently than in the original version. This is observed both for a large object in the frame - the planet, and for its satellite.

The threshold value was selected by subjective ranking. When analyzing a hundred images, it was determined that for the 2 × 2 blocks, the best results were obtained using a threshold value of 15.

Thus, in the work it was possible to improve the accuracy of the contour extraction in the manner suggested earlier. Recommendations are received regarding the choice of block size and threshold value. By subjective ranking it is established that at a threshold value of 15 for blocks of 2 × 2 size, the accuracy of contour allocation increases significantly. The tasks set in the work are solved, the goal is achieved.

Відомості про авторів

Мокріцький Вадим Анатолійович
Освіта: Повна вища, «Автоматика і телемеханіка» (1959).
Науковий ступінь: Доктор технічних наук (1983).
Вчене звання: Професор.
Місце роботи: Одеський національний політехнічний університет.
Область знань: Системи захисту інформації.
Наукові інтереси: Інформаційна безпека, Інформаційні технології проектування в електроніці та телекомунікація, обробка та аналіз томографічних зображень.
Email: *jyzel@rambler.ru*

Зорило Вікторія Вікторівна
Освіта: Повна вища, «Прикладна математика» (2004).
Науковий ступінь: Кандидат технічних наук.
Місце роботи: Одеський національний політехнічний університет.
Область знань: Системи захисту інформації.
Наукові інтереси: Захист інформації, обробка цифрових зображень.
Email: *jyzel@rambler.ru*

Ворнікова Марія Віталіївна
Освіта: Студентка магістратури Одеського національного політехнічного університету.
Email: *vornikovamasha@gmail.com*

Кремінський Владислав Юрійович
Освіта: Студент магістратури Одеського національного політехнічного університету.
Email: *vladnum5@gmail.com*

Личов Роман Володимирович
Освіта: Студент магістратури Одеського національного політехнічного університету.
Email: *romanlychov@gmail.com*

Матвеєва Анастасія Ігорівна
Освіта: Студентка магістратури Одеського національного політехнічного університету.
Email: *matveevanasty1@gmail.com*

Мурова Вероніка Володимирівна
Освіта: Студентка магістратури Одеського національного політехнічного університету.
Email: *murovanika@gmail.com*

Шпортюк Анастасія Геннадіївна
Освіта: Студентка магістратури Одеського національного політехнічного університету.
Email: *nanami2995@gmail.com*

УДК: 681.3.06

АЛГОРИТМИ ФАКТОРИЗАЦІЇ ТА ПЕРЕВІРКИ НЕЗВІДНОСТІ ПОЛІНОМІВ З ВИКОРИСТАННЯМ АПАРАТУ ЕЛІПТИЧНИХ КРИВИХ

Беспалов Олексій
КПІ ім. Ігоря Сікорського

ALGORITHMS FOR FACTORIZATION AND IRREDUCIBILITY TESTING OF POLYNOMIALS USING ELLIPTIC CURVES

Bespalov Oleksii
Igor Sikorsky Kyiv Polytechnic Institute

Анотація: **У статті сформульовані та обґрунтовані критерії незвідності полінома, які є узагальненнями аналогічних критеріїв для простоти числа. Особливо цікавим є узагальнення теореми Лєнстра, що забезпечує правильне обчислення кратних точок, які використовуються у алгоритмі Лєнстра. Доведення узагальнення цієї теореми у випадку поліномів над полем характеристики 2 повністю відрізняється від її доведення у класичному випадку і є дуже нетривіальним. Використовуючи побудовані критерії, розроблено ряд алгоритмів факторизації та перевірки незвідності поліномів над скінченним полем.**
Ключові слова: **Незвідні поліноми, еліптичні криві, теорема Лєнстри.**
Summary: **The article formulates and proves the criteria of the irreducibility of a polynomial, which are generalizations of similar criteria for the primality of the number. Of particular interest is the generalization of the Lenstra's theorem, which ensures the correct calculation of multiple points used in the Lenstra's algorithm. The proof of the generalization of this theorem in the case of polynomials over the field of characteristic 2 completely differs from the classical case and is very nontrivial.**
Using constructed criteria, we developed a number of algorithms for factorization and irreducibility tests of polynomials over a finite field. All of them are polynomial-time.
Keywords: **Invariant polynomials, elliptic curves, Lennister's theorem.**

Вступ

В різних прикладних задачах як симетричної, так і несиметричної криптографії використовуються незвідні поліноми з великими (до 700) степенями. Наприклад, найбільш поширеними методами побудови симетричних потокових шифрів, є використання лінійних рекурентних регістрів зсуву зі зворотнім зв'язком (ЛРР) та деякої нелінійної функції фільтрації [1], [2]. Кожен ЛРР описується деяким поліномом, алгебраїчні властивості якого тісно пов'язані з криптографічними властивостями як самого ЛРР, так і шифру в цілому. Зокрема, поліном обов'язково має бути незвідним.

У асиметричній криптографії незвідні поліноми також використовуються при побудові сучасних криптосистем на еліптичних кривих (див. наприклад, [3], [4] та їх бібліографію) для генерації базового поля.

Часто додатково буває необхідно, щоб степінь полінома n була простим числом. Така вимога також є природною і для симетричних, і для несиметричних криптосистем. У симетричних потокових шифрах, що використовують ЛРР, виконання цієї вимоги необхідно для отримання максимально можливого періоду вихідної гамми, що суттєво підвищує стійкість шифру до багатьох методів криптоаналізу (наприклад, до безключових методів, які можливі при наявності перекриття шифруючої гами). У несиметричних криптосистемах на еліптичних кривих саме така вимога є необхідною для відсутності субекспоненційних алгоритмів розв'язку

задачі DLP у групі точок еліптичної кривої [5].

Для перевірки незвідності поліномів використовується класичний детермінований алгоритм, що складається з $\left\lfloor \frac{n}{2} \right\rfloor$ кроків (див. наприклад, [6]). На кожному кроці виконується алгоритм Евкліда пошуку найбільшого спільного дільника поліномів степеня не менше n. Загалом такий алгоритм виконує близько $\frac{n^2}{2}$ ділень з залишком, що потребує значних часових затрат при великих n.

У роботі [7] було запропоновано імовірнісні алгоритми тестування незвідності поліномів та показано, що вони в багатьох випадках виявляються набагато ефективнішими за детермінований алгоритм, навіть при багатократному повторенні. Запропоновані імовірнісні алгоритми являють собою узагальнення відповідних імовірнісних алгоритмів для тестування простоти чисел [8], [9], [10]. Показано, що крім аналогів тестів Соловея-Штрассена и Міллера-Рабіна, для тестування незвідності поліномів може бути використаний аналог тесту Ферма, який є, взагалі кажучи, непридатним для тестування простоти числа. Наведено умови, за яких імовірність помилки даного тесту не перевищує ½. Також показано, що для тестування незвідності поліномів достатньо великих степенів (порядку 50 і більше), наведені імовірнісні тести є більш швидкодіючими, ніж класичний детермінований алгоритм. При цьому імовірність помилки тестів може бути зроблена як завгодно малою (наприклад, порядку 2×10^{-10}). Найбільш ефективними імовірнісні алгоритми тестування виявляються у випадку, коли степінь поліному є простим числом. Як було зазначено, ці алгоритми є певною мірою аналогами імовірнісних алгоритмів тестування простоти чисел, але повної аналогії не існує.

У [11] було представлено алгоритми розпізнавання поліномів Галуа над кільцями Галуа. Треба відмітити, що поліноми Галуа являють собою узагальнення незвідних поліномів над скінченими полями та відіграють ту ж роль, що й незвідні поліноми – вони використовуються для побудови розширень Галуа кілець Галуа так же, як незвідні поліноми використовуються для побудови розширень полів. Кільця Галуа є важливим об'єктом, який має досить багато застосувань як в теорії кодування [12], так і в криптографії, наприклад, в задачах розподілу таємниці [13]. Результати [11] продовжують та в деякому сенсі узагальнюють результати [7]. Крім того, у [11] побудовано декілька додаткових тестів, котрі також є імовірнісними та можуть використовуватися як для перевірки незвідності поліному над скінченим полем, так і для розпізнавання поліному Галуа над кільцем Галуа.

У цій роботі представлені результати досліджень, започаткованих у роботах [7], [11]. Зокрема, побудовані поліноміальні аналоги таких відомих алгоритмів перевірки простоти числа та факторизації чисел, як критерій Поклінгтона та $p-1$ метод Поларда. Але найбільш цікавими, принаймні з математичної точки зору, є поліноміальні аналоги алгоритмів Голдвассера-Кіліана-Аткіна та алгоритму Лєнстри, який використовують для факторизації поліномів апарату еліптичних кривих.

Значною перевагою алгоритмів факторизації, побудованих з використанням еліптичних кривих, є те, що у них замість групи $F_{p^n}^*$ використовується група точок еліптичної кривої $E \bmod p$. При цьому, якщо вибір еліптичної кривої виявився невдалим, то маємо змогу просто відкинути її та вибрати будь-яку іншу еліптичну криву E та базову точку на ній, бо групу $F_{p^n}^*$ перевибрати не можемо, оскільки вона єдина з точністю до ізоморфізму. Тому використання еліптичних кривих в таких алгоритмах надає нові можливості, як з математичної, так і з практичної точки зору.

Алгоритми Поклінгтона, Голдвассера-Кіліана-Аткіна та Поларда для перевірки незвідності та факторизації поліному

Узагальнений критерій незвідності Поклінгтона

Побудуємо критерій перевірки незвідності поліному, який є поліноміальним аналогом критерію Поклінгтона перевірки простоти числа [14]. Спочатку сформулюємо та доведемо твердження, необхідне для побудови цього критерію.

Нехай $f(x) \in F_p[x]$ – незвідний, $\deg f = n$. Нехай існує просте $q|p^n - 1$, таке, що $q > p^{\frac{n}{2}} - 1$.

Теорема 1: якщо існує поліном $a(x) \in F_p[x]$, такий, що:

1) $a(x)^{p^n-1} \equiv 1 (\mathrm{mod}\, f)$;

2) $\left(a(x)^{\frac{p^n-1}{q}} - 1, f(x)\right) = 1$,

то $f(x)$ – незвідний.

Доведення. Нехай $f(x)$ – звідний, тобто існує такий поліном $g(x)$, що $g(x)|f(x)$ та $g(x)$ – незвідний і $\deg g(x) = s \leq \frac{n}{2}$. Тоді $p^s - 1 \leq p^{\frac{n}{2}} - 1 < q$, отже, $(p^s - 1, q) = 1$ і $\exists u: uq = 1 (\mathrm{mod}\, p^s - 1)$.

Тоді

$a(x)^{\frac{p^n-1}{q}} \equiv a(x)^{\frac{p^n-1}{q}} \big(\mathrm{mod}\, g(x)\big) \equiv a(x)^{u(p^n-1)} \big(\mathrm{mod}\, g(x)\big)$, а за умовою 1) $a(x)^{p^n-1} \equiv 1 (\mathrm{mod}\, f)$, тобто $a(x)^{u(p^n-1)} \equiv 1 (\mathrm{mod}\, g)$, так як $g(x)|f(x)$.

Останнє означає, що $a(x)^{\frac{p^n-1}{q}} - 1$, ділиться на $g(x)$, тобто $\left(a(x)^{\frac{p^n-1}{q}} - 1, f(x)\right) \neq 1$, що суперечить умові 2). Теорему доведено.

Отриманий результат дозволяє побудувати наступний алгоритм перевірки незвідності полінома, який назвемо алгоритмом Поклінгтона.

Алгоритм Поклінгтона перевірки незвідності полінома

Вхід: p – просте число, $f(x) \in F_p[x], \deg f = n: q$ – просте, $q|p^n - 1, q \geq p^{\frac{n}{2}} - 1$.

1. Вибрати випадковий поліном $a(x) \in F_p[x],\ \deg a > 1$.
2. Обчислити $d = \big(a(x), f(x)\big)$. Якщо $d \neq 1$, то робимо висновок, що $f(x)$ - звідний і закінчуємо роботу алгоритма.
3. Обчислити $d_1 = a(x)^{p^n-1} \bmod f(x)$. Якщо $d_1 \neq 1$, то робимо висновок, що $f(x)$ - звідний і закінчуємо роботу алгоритма.
4. Обчислити $d_2 = \left(a(x)^{\frac{p^n-1}{q}} - 1, f(x)\right)$. Якщо $d_2 \neq 1$, то робимо висновок, що $f(x)$ - звідний і закінчуємо роботу алгоритма.

Інакше робимо висновок, що $f(x)$ – незвідний і закінчуємо роботу алгоритма.

Аналіз часу роботи алгоритму: після того, як знайдено число q з необхідними властивостями, цей алгоритм виконує три алгоритми Евкліда замість n, як в класичному алгоритмі перевірки незвідності.

Узагальнений критерій перевірки незвідності Голдвассера-Кіліана-Аткіна

Побудуємо еліптичний аналог алгоритму Голдвассера, Кіліана та Аткіна перевірки незвідності поліному (класичний алгоритм було запропоновано у [15]). Для цього необхідно довести наступну теорему.

Нехай $f(x) \in F_p[x], \deg f = n$, а E – множина точок $F_{p^n} \otimes F_{p^n}$, яка задана рівнянням $y^2 = u^3 + au + b \big(\mathrm{mod}\, f(x)\big)$. Нехай m – деяке ціле число. Припустимо, що існує таке просте число $q|m$, що $q > \left(p^{\frac{n}{4}} + 1\right)^2$. Тоді справедлива наступна теорема.

Теорема 2: якщо існує така точка $P \in E$, що

1) $mP = O$;

2) точка $(\frac{m}{q})P$ – визначена і не дорівнює O,

то $f(x)$ – незвідний.

Доведення. Якщо $f(x)$ – звідний, то існує поліном $g(x)|f(x)$ такий, що $g(x)$ – незвідний і $\deg g(x) = s \leq \frac{n}{2}$. Нехай E' –

еліптична крива над F_{p^s} (де поле F_{p^s} побудовано як факторкільце за ідеалом $\big(g(x)\big)$ і всі точки кривої E' отримані з точок кривої E редукцією їхніх координат за модулем$g(x)$). Нехай m' – порядок кривої E'.

За теоремою Хасе, $m' \le p^s + 1 + 2\sqrt{p^s} = \left(p^{\frac{s}{2}} + 1\right)^2 < q$, звідки $(m', q) = 1$. Отже, існує таке u: $uq \equiv 1 (\mathrm{mod}\ \mathrm{m}')$.

Нехай $P' \in E'$ – «проекція» точки $P \in E$ на еліптичну криву E' (тобто координати точки P приведені за $\mathrm{mod}\ g(x)$). Тоді на E' виконується рівність

$$\frac{m}{q}P' = uq\frac{m}{q}P' = umP'.$$

Але, за умовою 1), $umP = O$, звідки $umP' = O$, тобто $\left(\frac{m}{q}\right)P' = O$ та x-координата точки $\left(\frac{m}{q}\right)P'$ ділиться на $g(x)$. Далі, за умовою 2), $\left(\frac{m}{q}\right)P \neq O$, звідки x-координата точки $\left(\frac{m}{q}\right)P$ взаємно проста з $f(x)$. Тоді x-координата точки $\left(\frac{m}{q}\right)P$ також взаємно проста з $g(x)$, звідки $\left(\frac{m}{q}\right)P' \neq O$, що суперечить висновку вище. Теорему доведено.

Спираючись на цей результат можна побудувати наступний алгоритм перевірки незвідності, який назвемо еліптичним алгоритмом Голдвассера-Кіліана-Аткіна.

Алгоритм Голдвассера-Кіліана-Аткіна перевірки незвідності полінома

Вхід: $f(x) \in F_p[x], \deg f = n$.

1. Вибрати випадкові поліноми $a(x) \in F_p[x]$, $u(x) \in F_p[x]$, $y(x) \in F_p[x]$, так, що $\deg a < n$, $\deg u < n$, $\deg y < n$.

2. Обчислити $b(x) = [y(x)^2 - u(x)^3 - a(x)u(x)] \bmod f(x)$. Пара значень (u, y) буде представляти точку кривої $E\big(F_{p^n}\big)$, яка задана рівнянням $y^2 = u^3 + au + b(\mathrm{mod}\ f(x))$.

3. Якщо крива E сингулярна, то повертаємось до пункту 1.

4. Використовуючи алгоритм Шенкса або Скуфа [16], обчислити порядок m кривої E.

5. Якщо в процесі роботи алгоритму отримано необчислюємий вираз, то робимо висновок, що $f(x)$ звідний та закінчуємо роботу алгоритму.

6. Якщо m не подається у вигляді $m = kq$, де k – невелике ціле число (як привило, $k = 2$ або $k = 4$), а q – просте, то повертаємось до пункту 1.

7. Обчислити $Q_1 = mP$ і $Q_2 = kP$.

8. Якщо в процесі отримано необчислюємий вираз (тобто виникає ділення на ноль), то робимо висновок, що $f(x)$ – звідний та закінчуємо роботу алгоритму.

9. Якщо $Q_1 \neq O$, то робимо висновок, що $f(x)$ – звідний та закінчуємо роботу алгоритму.

10. Якщо $Q_2 = O$, то повертаємось до пункту 1. В іншому випадку робимо висновок, що $f(x)$ – незвідний та закінчуємо роботу алгоритму.

Аналіз часу роботи алгоритму: для того, щоб зменшити час, витрачений на метод Скуфа [16], А.О.Л. Аткін запропонував (для алгоритму тестування простоти числа) будувати криву спеціального вигляду. Та у випадку перевірки незвідності поліному цей алгоритм не швидший за класичний, тому є цікавим лише з математичної точки зору.

Узагальнений p-1 метод Полларда перевірки незвідності полінома

Побудуємо поліноміальний аналог $p - 1$ – методу Полларда [17] розкладу на прості множники. Цей алгоритм не тільки перевіряє незвідність поліному, але й у випадку його звідності видає якийсь з його нетривіальних дільників. Слід зазначити, що алгоритми 1 та 2 також можна модифікувати так, щоб в результаті їх роботи отримувати нетривіальні дільники звідного поліному.

Нехай $f(x) \in F_p[x]$ – звідний поліном (з невідомим розкладом на незвідні), $\deg f = n$.

Нехай відомо, що деякий (невідомий) поліном $g(x) \in F_p[x]$, $g(x) | f(x)$, з $\deg g = s$ (невідомо) володіє наступною

властивістю: в розкладі p^s-1 на прості множники всі степені простих не перевищують деякого (відомого) числа $B \in Z$, тобто $p^s-1=\prod_{i=1}^{n} q_i^{a_i}$, де $\forall i=\overline{1,l}: q_i^{a_i} \le B$.

Позначимо через $k=k(B)$ НСК всіх цілих чисел від 1 до B: $k=\text{НСК}(1,2,\dots,B)$. Очевидно $\forall i=\overline{1,l}: k \vdots q_i^{a_i}$, тобто $k \vdots p^s-1$. Тоді, так як для будь-якого $a(x) \in F_p[x]$, такого, що $\big(a(x),f(x)\big)=1$, виконується: $a(x)^{p^s-1} \equiv 1\big(\mathrm{mod}\, g(x)\big)$, то $a(x)^k \equiv 1\big(\mathrm{mod}\, g(x)\big)$, це значить, що $(a(x)^k-1) \bmod f(x) \vdots g(x)$.

Алгоритм перевірки незвідності полінома та знаходження нетривіального дільника з використанням p-1-методу Полларда

Вхід: $f(x) \in F_p[x];\ B \in Z$.

1. Обчислити $k=\text{НСК}(1,2,\dots,B)$.
2. Вибрати $a(x) \in F_p[x]$ таке, що $\deg a < n$.
3. Обчислити $d(x)=\big(a(x),f(x)\big)$.
4. Якщо $\deg d(x)>1$, то $d(x)$ – нетривіальний дільник $f(x)$. В цьому випадку алгоритм закінчує роботу та видає цей нетривіальний дільник полінома.
5. Обчислити $g(x)=a(x)^k \bmod f(x)$.
6. Якщо $g(x)=1$, то повертаємось до пункту 2.
7. Обчислити $u(x)=\big(g(x)-1,f(x)\big)$.
8. Якщо $\deg u(x) \ge 1$, то $u(x)$ – нетривіальний дільник $f(x)$. Алгоритм закінчує роботу і видає цей дільник. Інакше робимо висновок, що $f(x)$ –незвідний та закінчуємо роботу алгоритму.

Аналіз часу роботи алгоритму: час роботи алгоритму, а також і імовірність успіху, залежать від вибору параметра $B \in Z$, який визначається обчислювальними можливостями користувача. Цей алгоритм також не є швидшим за класичний.

Теореми Лєнстра та алгоритм Лєнстра

Класичний (числовий) алгоритм Ленстра [18-20] належить до класу субекспоненціальних алгоритмів факторизації. Проводячи порівняння алгоритму Ленстра з методом квадратичного решета (QS) та методом решета числового поля (NFS) бачимо, що все залежить від розміру найменшого дільника числа n. Якщо число n було обрано згідно з методом RSA в якості добутку двох простих чисел приблизно однакової довжини, то метод Ленстра має таку ж швидкодію, що й метод квадратичного решета, але поступається методу решета числового поля.

Але якщо число n має довжину, значно більшу за існуючі показники для методів QS та NFS (останнім найбільшим розкладом чисел RSA з використанням NFS є число довжини 768 біт), то знаходження дільника числа n можливе лише з використанням методу, що базується на використанні апарату еліптичних кривих.

Нехай найменший множник числа n дорівнює p. Тоді час роботи алгоритму Ленстра можена оцінити величиною:

$$\exp\big(\sqrt{2}+o(1)\sqrt{ln\,p\,ln\,ln\,p}\big),$$

яка буде справедливою для випадку, коли межу B було обрано близькою до величини

$$\exp\frac{\sqrt{2}}{2}+o(1)\sqrt{\ln p \ln\ln p}.$$

Так як значення множника p нам невідомо, то вибір величини параметру алгоритму B відбувається емпірично. Це погіршує практичну оцінку збіжності методу Ленстра. Зазначимо, що процес обчислення кратних точок у алгоритмі зберігає загальну асимптотичну оцінку, хоча забезпечує досить великий практичний приріст швидкості збіжності алгоритму.

Алгоритм Лєнстра використовує знаходження кратних точок kP для точки P еліптичної кривої. Ця операція, з використанням методу Горнера, виконується за $O(\log k)$ кроків. Будемо розглядати точку P і всі її кратні точки за модулем деякого поліному $g(x)$. Кожен раз при обчисленні кратної точки kP фактично будемо обчислювати її координати по модулю $g(x)$. Для того, щоб всі ці обчислення були коректними, потрібно щоб виконувалась наступна умова: всі

знаменники координат точок повинні бути взаємно прості з $g(x)$.

Спочатку розглянемо випадок $f(x) \in F_p[x]$, де $p > 3$. Нехай $f(x) \in F_p[x]$ – звідний поліном, $\deg f(x) = n$. Нехай деяка еліптична крива над кільцем поліномів $F_p[x]$ задається рівнянням $y^2 = x^3 + ax + b, \quad a, b, \in F_p[x]$. Нехай $\Delta = 4a^3 + 27b^2 \neq 0$ та $4a^3 + 27b^2$ не має з $f(x)$ спільних дільників (тоді $x^3 + ax + b$ не має кратних коренів за модулем $g(x)$ для будь-якого простого дільника $g(x)$ полінома $f(x)$). На практиці, вибираючи коефіцієнти a, b, ми перевіряємо, чому дорівнює НСД $\left(4a^3 + 27b^2, f(x)\right)$. Якщо результат більше 1, то ми знайшли нетривіальний дільник $f(x)$ і задача вирішена. Далі будемо припускати, що НСД $\left(4a^3 + 27b^2, f(x)\right) = 1$.

Для точок $P_1, P_2 \in E$, де $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$, їх сума $P_3 = (x_3, y_3)$ обчислюється за наступним правилом:

$$\begin{aligned} x_3 &= \left(\frac{3x_1^2 + a}{2x_1}\right)^2 - 2x_1, \\ y_3 &= -y_1 + \left(\frac{3x_1^2 + a}{2x_1}\right)(x_1 - x_3) \end{aligned} \tag{1}$$

якщо $P_1 \neq P_2$, та за правилом:

$$\begin{aligned} x_3 &= \left(\frac{3x_1^2 + a}{2x_1}\right)^2 - 2x_1, \\ y_3 &= -y_1 + \left(\frac{3x_1^2 + a}{2x_1}\right)(x_1 - x_3) \end{aligned} \tag{2}$$

якщо $P_1 = P_2$.

Теорема 3 (теорема Лєнстра для $p > 3$): нехай E – еліптична крива, яка описується рівнянням:

$$y^2 = x^3 + ax + b, \; a, b \in F_p[x],$$

і НСД $(4a^3 + 27b^2, n) = 1$. Нехай P_1 та P_2 – дві точки на E, у яких знаменники координат взаємно прості з $f(x)$, та $P_1 \neq -P_2$. Тоді точка $P_1 + P_2 \in E$, отримана за формулами (1), має координати, в яких знаменники взаємно прості з $f(x)$, тоді і тільки тоді, коли у $f(x)$ немає незвідного дільника $g(x)$, для якого сума точок $P_1(\mathrm{mod}\, g(x))$ і $P_2(\mathrm{mod}\, g(x))$ на еліптичній кривій $E(\mathrm{mod}\, g(x))$ дорівнювала б точці на нескінченності $O(\mathrm{mod}\, g(x)) \in E(\mathrm{mod}\, g(x))$.

Зауваження: тут $E(\mathrm{mod}\, g(x))$ позначає еліптичну криву над полем $F_p[x]/(g(x))$.

Доведення: спершу припустимо, що всі точки $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$, та $P_1 + P_2 \in E$ мають координати, знаменники яких взаємно прості з $f(x)$. Необхідно довести, що для будь-якого незвідного дільника $g(x)$ полінома $f(x)$ сума $P_1(\mathrm{mod}\, g(x)) + P_2(\mathrm{mod}\, g(x)) \neq O(\mathrm{mod}\, g(x))$.

Якщо $x_1 \neq x_2(\mathrm{mod}\, g(x))$, то з визначення операції додавання точок на $E(\mathrm{mod}\, g(x))$ одразу випливає, що $P_1(mod\; g(x)) + P_2(mod\; g(x)) \neq O(mod\; g(x))$.

Тепер припустимо, що $x_1 \equiv x_2(mod\; g(x))$. При $P_1 = P_2$ координати точки $P_1 + P_2 = 2P_1$ визначаються формулами (2), в яких кожний член замінюється його лишком за модулем $g(x)$. Необхідно показати, що знаменник $2y_i$ дробу в правій частині (2) не ділиться на $g(x)$. Але, якби він ділився на $g(x)$, то і вираз $3x_1^2 + a$ ділився б на $g(x)$. Тоді x_1 був би коренем за модулем $g(x)$ як многочлена $x^3 + ax + b$, так і його похідної $3x^2 + a$. Але це суперечить припущенню, що у даного многочлена відсутні кратні корені за модулем $g(x)$. Нехай $P_1 \neq P_2$ і координати точки $P_1 + P_2 = P_3$ визначаються за формулами (1). Так як $x_1 \equiv x_2(mod\; g(x))$, а $x_1 \neq x_2$, то можна записати $x_2 = x_1 + g(x)^r x$, де $r \geq 1$ вибрано так, що ні чисельник, ні знаменник x не діляться на $g(x)$. За припущенням знаменники координат точки $P_1 + P_2$ не діляться на $g(x)$. Тому із формул (1) випливає, що $y_2 = y_1 + g(x)^r y$. З іншого боку,

$$\begin{aligned} y_2^2 &= (x_1 + g(x)^r x)^3 + \\ &+ a(x_1 + g(x)^r x) + b \equiv \\ &\equiv x_1^3 + ax_1 + b + \\ &+ g(x)^r x(3x_1^2 + a) \equiv \\ &\equiv y_1^2 + g(x)^r x(3x_1^2 + a) \\ &(mod\; g(x)^{r+1}). \end{aligned} \tag{3}$$

Оскільки $x_2 \equiv x_1 (mod\ g(x))$ та $y_2 \equiv y_1 (mod\ g(x))$, то $P_1 (mod\ g(x)) \equiv P_2 (mod\ g(x))$, тобто $P_1 (mod\ g(x)) + P_2 (mod\ g(x)) = 2P_1 (mod\ g(x))$.

Очевидно, що $2P_1 (mod\ g(x)) = O (mod\ g(x))$ тоді і тільки тоді, коли $y_1 \equiv y_2 \equiv O (mod\ g(x))$. Але якби це рівняння виконувалось, то тоді вираз

$$y_2^2 - y_1^2 = (y_2 - y_1)(y_2 + y_1)$$

повинен був би ділитися на $g(x)^{r+1}$ (тобто повинен ділитися на $g(x)^{r+1}$ чисельник цього виразу). В цьому випадку із (3) випливало б, що $3x_1^2 + a \equiv O (mod\ g(x))$. Але це неможливо, оскільки $x^3 + ax + b$ не має кратних коренів за модулем $g(x)$. Тобто x_1 не може бути загальним коренем цього многочлена і його похідної. Значить, $P_1 (mod\ g(x)) + P_2 (mod\ g(x)) \neq$ $\neq O (mod\ g(x))$, що й треба було довести.

Доведемо твердження у зворотний бік. Нехай $P_1 (mod\ g(x)) + P_2 (mod\ g(x)) \neq O (mod\ g(x))$ для кожного незвідного дільника $g(x)$ полінома $f(x)$. Фіксуємо деякий поліном $g(x)|f(x)$. Формули (1) та (2) показують, що якщо $x_2 \neq x_1 (mod\ g(x))$, то знаменників, які діляться на $g(x)$,, у виразах для координат суми точок немає. Тому припустимо, що $x_2 \equiv x_1 (mod\ g(x))$. Тоді $y_2 \equiv \pm y_1 (mod\ g(x))$, але так як $P_1 (mod\ g(x)) + P_2 (mod\ g(x)) \neq$ $O (mod\ g(x))$, то $y_2 \equiv y_1 \neq O (mod\ g(x))$. При $P_2 = P_1$ з формули (2) разом з умовою $y_1 \neq O (mod\ g(x))$ слідує, що знаменники координат точки $P_1 + P_2 = 2P_1$ взаємно прості з $g(x)$. Якщо $P_2 \neq P_1$, знову записуємо x_2 у вигляді $x_2 = x_1 + p^r x$, де x не ділиться на $g(x)$, і використовуючи рівняння (3), отримуємо $\frac{y_2^2 - y_1^2}{x_2 - x_1} \equiv 3x_1^2 + a (mod\ g(x))$. Так як $g(x)$ не ділить $y_1 = y_2 \equiv 2y_1 (mod\ g(x))$, то звідси випливає, що знаменник виразу $\frac{(y_2^2 - y_1^2)}{(y_1 + y_2)(x_2 - x_1)} = \frac{y_2 - y_1}{x_2 - x_1}$ не ділиться на $g(x)$ і в силу формул (2) знаменники координат точки $P_1 + P_2$ не діляться на $g(x)$. Теорема доведена.

Нехай тепер E – еліптична крива над полем F_{2^n}, яка описується рівнянням:

$$y^2 + xy = x^3 + ax^2 + b, \qquad b \neq 0$$

Для її точок $P_1, P_2 \in E$, де $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$, їх сума $P_3 = (x_3, y_3)$ обчислюється за наступним правилом:

$$\begin{aligned} x_3 &= \left(\frac{y_2 + y_1}{x_2 + x_1}\right)^2 + \left(\frac{y_2 + y_1}{x_2 + x_1}\right) + x_1 + x_2 + a, \\ y_3 &= y_1 + \left(\frac{y_2 + y_1}{x_2 + x_1}\right)(x_1 + x_3) + x_3, \end{aligned} \tag{4}$$

якщо $P_1 \neq P_2$, та за правилом

$$\begin{aligned} x_3 &= x_1^2 + \frac{b}{x_1^2}, \\ y_3 &= x_1^2 + \frac{x_1^2 + y_1}{x_1} x_3 + x_3, \end{aligned} \tag{5}$$

якщо $P_1 = P_2$.

Теорема 4 (теорема Лєнстра для $p = 2$): нехай E – еліптична крива, яка описується рівнянням: $y^2 + xy = x^3 + ax^2 + b,\ b \neq 0$. Позначимо через $f(x) \in F_2[x]$ – звідний поліном, $\deg f(x) = n$, а також $(b(x), f(x)) = 1$.

Нехай P_1 та P_2 – дві точки на E, у яких знаменники координат взаємно прості з $f(x)$ та $P_1 \neq -P_2$, а $P_1 + P_2 \in E$ має координати, у яких знаменники взаємно прості з $f(x)$. Тоді для будь-якого незвідного $g(x)$, такого що $g(x)|f(x)$, виконується:

$P_1 (mod\ g(x)) + P_2 (mod\ g(x)) \neq$ $O (mod\ g(x))$.

Доведення: розглянемо два випадки.

1. Нехай $x_1 \neq x_2 (mod\ g(x))$.

Тоді $P_1 (mod\ g(x)) \neq P_2 (mod\ g(x))$ і додавання цих точок виконується за формулою (4).

Тоді знаменник у першій координаті $P_1 + P_2$ дорівнює $x_2^2 + x_1^2 = (x_1 + x_2)^2 \neq O (mod\ g(x))$, отже $P_1 (mod\ g(x)) + P_2 (mod\ g(x)) \neq O (mod\ g(x))$.

2. Нехай тепер $x_1 \equiv x_2 (mod\ g(x))$. Можливі два випадки.

Випадок 2а. Нехай $P_1 = P_2$.

В такому випадку справедлива рівність $P_1(mod\ g(x)) \neq P_2(mod\ g(x))$ та додавання точок $P_1 + P_2$ і $P_1(mod\ g(x)) + P_2(mod\ g(x))$ ми будемо обраховувати згідно з формулою (5).

Доведемо від супротивного. Припустимо, що $P_1(mod\ g(x)) + P_2(mod\ g(x)) = O(mod\ g(x))$, а отже $x_1(mod\ g(x)) = 0$. Так як знаменник суми $P_1 + P_2$ не ділиться на $g(x)$, то чисельник повинен ділитися на $g(x)$, тобто $b \vdots g(x)$, а звідси випливає, що $(b(x), f(x)) \neq 1$, що суперечить умові теореми. Отже $x_1(mod\ g(x) \neq 0$, та $P_1(mod\ g(x)) + P_2(mod\ g(x)) \neq O(mod\ g(x))$.

Випадок 2б. Нехай $P_1 \neq P_2$, але $P_1(mod\ g(x)) = P_2(mod\ g(x))$, тобто $x_1 \equiv x_2(mod\ g(x))$.

Для обчислення суми $P_1 + P_2$ будемо використовувати формулу (5). Тоді запишемо x_2 у вигляді $x_2 = x_1 + g(x)^r x$, де $(x, g(x)) = 1$, та $y_2 = y_1 + g(x)^r y$.

Так як $P_1(mod\ g(x)) = P_2(mod\ g(x))$, то для обчислень $P_1(mod\ g(x)) + P_2(mod\ g(x))$ будемо використовувати формулу (4).

Доведемо, що знаменник виразу $2P_1(mod\ g(x)) \neq O(mod\ g(x))$, тобто що x_1 не ділиться на $g(x)$.

Доводимо від супротивного. Якщо $x_1 \vdots g(x)$, то згідно з (5), $x_2 \vdots g(x)$.

Справедлива наступна рівність: $y_1^2 + y_2^2 = y_1^2 + y_2^2 + g(x)^{2r} y^2$, тобто $(y_1^2 + y_2^2) \vdots g(x)^{2r} \vdots g(x)^{r+1}$.

З іншого боку,

$$\begin{gathered} y_2^2 + y_1^2 = x_1 y_1 + x_2 y_2 + x_1^3 + \\ + a(x_1^2 + x_2^2) = g(x)^r x y_1 + \\ + g(x)^r x_1 y + g(x)^{2r} xy + \\ + (x_1 + x_2)(x_1^2 + x_1 x_2 + x_2^2) + \\ + a g(x)^{2r} x^2 = g(x)^r x y_1 + \\ + g(x)^r x_1 y + g(x)^{2r} xy + \\ + g(x)^r x(x_1^2 + x_1 x_2 + x_2^2) + \\ + a g(x)^{2r} x^2. \end{gathered} \tag{6}$$

Бачимо, що кожен доданок в правій частині рівності (6) ділиться на $g(x)^{r+1}$, окрім $g(x)^r x y_1$. А так як ліва частина рівності теж ділиться на $g(x)^{r+1}$, то доданок $g(x)^r x y_1$ теж повинен ділитися на $g(x)^{r+1}$. З визначення маємо, що $(x, g(x)) = 1$, а звідси випливає, що $y_1 \vdots g(x)$.

Якщо $x_1 \equiv O(mod\ g(x))$, то з рівняння кривої $y_1 \equiv b(mod\ g(x))$. Звідси випливає, що $b \vdots g(x)$. Це означає, що $(b, f(x)) \neq 1$ і є протиріччям нашому припущенню.

І навпаки, нехай для кожного $g(x)$, яке ділить поліном $f(x)$, виконується наступне:

$$\begin{gathered} P_1(mod\ g(x)) + P_2(mod\ g(x)) \\ \neq O(mod\ g(x)). \end{gathered} \tag{7}$$

Доведемо, що у координат суми $P_1 + P_2$ знаменник не ділиться на $g(x)$.

Розглянемо два випадки.

1. Нехай $x_1 \neq x_2(mod\ g(x))$. Тоді $P_1 \neq P_2$, $P_1(mod\ g(x)) \neq P_2(mod\ g(x))$, а додавання точок будемо обчислювати за формулою (3). Так як $P_1(mod\ g(x)) + P_2(mod\ g(x)) \neq O(mod\ g(x))$, то $(x_1^2 + x_2^2)\ mod\ g(x) \neq O(mod\ g(x))$. Звідси випливає, що знаменник $(x_1^2 + x_2^2)$ не ділиться на $g(x)$, що й треба було довести.

2. Розглянемо протилежний випадок. Тут також можливі варіанти.

2а. Нехай $x_1 \equiv x_2(mod\ g(x))$. Тоді є два варіанти, $P_1(mod\ g(x)) = P_2(mod\ g(x))$ або $P_1(mod\ g(x)) = -P_2(mod\ g(x))$. Другого варіанту бути не може, так як згідно з (7) $P_1(mod\ g(x)) + P_2(mod\ g(x)) \neq \neq O(mod\ g(x))$. Залишається умова, що $P_1(mod\ g(x)) = P_2(mod\ g(x))$ та $y_1 \equiv \equiv y_2(mod\ g(x))$. З (7) маємо $2P_1(mod\ g(x)) \neq O(mod\ g(x))$ і тоді $x_1(mod\ g(x)) \neq O(mod\ g(x))$ або $b \vdots g(x)$, а це суперечить умові теореми. Це значить, що $(x_1, g(x)) = 1$. Тоді, якщо $P_1 = P_2$, то знаменники координат суми $P_1 + P_2$, які відповідно рівні x_1 та x_2, взаємно прості з $g(x)$, що й потрібно було довести.

2б. Нехай $P_1 \neq P_2$, але $x_1 \equiv \equiv x_2(mod\ g(x))$ та $y_1 \equiv y_2(mod\ g(x))$. В цьому випадку суму $P_1 + P_2$ обчислюємо за формулою (5). Також ми знаємо, що

$x_1(mod\ g(x)) \neq O(mod\ g(x))$. Покажемо, що якщо $x_1 + x_2 \vdots g(x)^r$, то і $y_1 + y_2 \vdots g(x)^r$. Запишемо x_2 у вигляді $x_2 = x_1 + xg(x)^r$, де $(x, g(x)) = 1$. Тоді з рівняння кривої можемо записати

$$\begin{aligned} y_1^2 + y_2^2 &= x_1y_1 + x_2y_2 + x_1^3 + x_2^3 \\ &+a(x_1^2 + x_2^2) = \\ &= x_1y_1 + x_1y_2 + y_2x_1 + y_2x_2 + \\ &+a(x_1^2 + x_2^2) + (x_1 + x_2) + \\ &(x_1^2 + x_1x_2 + x_2^2) = \\ &= x_1(y_1 + y_2) + y_2(x_1 + x_2) + \\ &+a(x_1^2 + x_2^2) + \\ &+(x_1 + x_2)(x_1^2 + x_1x_2 + x_2^2). \end{aligned} \quad (8)$$

Відомо, що в (8) доданки $(x_1 + x_2)(x_1^2 + + x_1x_2 + x_2^2)$ та $y_2(x_1 + x_2)$ діляться на $g(x)^r$, а $a(x_1^2 + x_2^2)$ ділиться на $g(x)^{2r}$, отже можемо зробити висновок, що сума $y_1^2 + y_2^2 + x_1(y_1 + y_2)$ ділиться на $g(x)^r$. Запишемо цю суму у вигляді двох множників $(y_1 + y_2)(y_1 + y_2 + x_1)$. З того, що один із них не ділиться на $g(x)^r$, випливає, що $(y_1 + y_2)$ ділиться на $g(x)^r$. Це й треба було довести.

Використаємо доведені теореми для побудови поліноміального аналогу алгоритму Лєнстра.

Нехай $f(x) \in F_p[x]$ – звідний поліном, розклад якого потрібно знайти та $\deg f(x) = n$.

Нехай є метод породження пар (E, P) – еліптичної кривої та точки на ній. Ця еліптична крива має вид $y_2 = x_3 + ax + b$, $a, b \in F_p[x]$, а точка $P = (x, y) \in E$. Маючи таку пару використовуємо нижче приведений алгоритм. Якщо за допомогою цієї процедури не вдається отримати нетривіальний дільник полінома $f(x)$, то утворюємо нову пару (E, P) та повторюємо алгоритм спочатку.

До того, як почати працювати з кривою E за модулем $f(x)$, потрібно перевірити, що це дійсно еліптична крива по модулю будь-якого $g(x)|f(x)$, тобто, що многочлен у правій частині рівняння не має кратних коренів за модулем $g(x)$. Ця умова виконується тоді і тільки тоді, коли дискримінант $4a^3 + 27b^2$ взаємно простий з $f(x)$. Таким чином, необхідною умовою є НСД $(4a^3 + 27b^2, f(x)) = 1$. Звичайно, якщо НСД не дорівнює 1 або $f(x)$, то отримуємо дільник полінома $f(x)$. Якщо цей НСД дорівнює $f(x)$, то слід обрати іншу еліптичну криву.

Далі припустимо, що вибрали два натуральних числа B і C. Тут B – максимальна величина простого дільника цілого числа k, на яке необхідно множити точку P. Чим більше B, тим більша ймовірність того, що $kP(\mathrm{mod}\ g(x)) = O(\mathrm{mod}\ g(x))$ для пари (E, P) і деякого $g(x)|f(x)$. З іншого боку, чим більше B, тим довше доведеться обчислювати $kP(\mathrm{mod}\ g(x))$. Тому B потрібно вибирати таким чином, щоб мінімізувати час роботи. Число повинно служити верхньою межею для незвідного дільника $g(x)|f(x)$, з яким необхідно отримати співвідношення $kP(\mathrm{mod}\ g(x)) = O(\mathrm{mod}\ g(x))$. Потім вибираємо k за формулою

$$k = \prod_{l \leq B} l^{a_l},$$

тобто подаємо його у вигляді добутку степенів простих чисел, що не перевершують B, кожна з яких не перевершує C. Тоді, згідно теореми Хассе, якщо $p + 1 + 2\sqrt{p} < C$ і порядок кривої $E(\mathrm{mod}\ g(x))$ не ділиться ні на яке просте число, більше B, то k кратне цьому порядку і тому $kP(\mathrm{mod}\ g(x)) = O(\mathrm{mod}\ g(x))$.

Працюючи за модулем $f(x)$ обчислюємо kP таким чином. Використовуючи метод повторного подвоєння, знаходимо $2,2(2P), 2(4P), \dots, 2^{a_2}P$, потім $3(2^{a_2})P, 3(3(2^{a_2})P), \dots, 3^{a_3}2^{a_2}P$ і т.д., поки не отримаємо $\prod_{l \leq B} l^{a_l}P$ (множимо, послідовно переходячи від найменших простих дільників ι числа k до найбільших). У цих обчисленнях, при кожному діленні по модулю $f(x)$ застосовуємо алгоритм Евкліда для знаходження оберненого елемента. Якщо на якійсь стадії алгоритм Евкліда не дає оберненого елемента, то або знайдений дільник $f(x)$ нетривіальний або НСД $f(x)$ і цього знаменника дорівнює $f(x)$. В останньому випадку слід повернутися до початку і обрати іншу пару (E, P). Якщо алгоритм Евкліда завжди дає зворотній елемент і таким чином обчислюється $kP(\mathrm{mod}\ g(x))$, слід повернутися до початку і обрати іншу пару (E, P).

Висновки

У даній роботі були розглянуті не зовсім звичні способи застосування еліптичних кривих – не для побудови криптосистем, а для перевірки незвідності поліномів над скінченним полем та для їх факторизації. Були запропоновані методи, які є поліноміальними узагальненнями відомих методів перевірки простоти чисел та розкладу числа на прості множники.

Для обґрунтування цих методів було узагальнено деякі теореми з теорії чисел. Особливий інтерес представляє узагальнення теореми Лєнстра, що забезпечує правильне обчислення кратних точок, які використовуються у алгоритмі Лєнстра. Зазначимо, що ця теорема є нетривіальною навіть у випадку кільця цілих чисел.

Базуючись на отриманих результатах, запропоновано ряд алгоритмів факторизації та перевірки незвідності поліномів над скінченним полем. Дані алгоритми побудовані на основі вже відомих критеріїв простоти та алгоритмів розкладу на множники чисел, що допомагає зберегти їх доступність та зрозумілість. Основною перевагою даних алгоритмів є використання абелевих груп, які побудовані на еліптичних кривих. Дійсно, існує великий вибір різних еліптичних кривих над заданим полем із різними порядками. Тому є можливість переобрати криву, якщо її вибір виявився невдалим. Хоча ці алгоритми і не дають суттєвої переваги у швидкодії, як і їх прообрази – алгоритми факторизації чисел, але вони демонструють нові підходи до вирішення давно існуючої та актуальної задачі перевірки незвідності полінома, а також є досить цікавими з точки зору математики.

Перелік посилань

[1] М. Глухов. И. Круглов. А. Пичкур, А. Черёмушкин, *Введение в теоретико-числовые методы криптографии* // СПб.: Изд-во "Лань", 2011г., 400с.

[2] Л. А. Завадская, *Потоковые системы шифрования, основанные на регистрах сдвига* // Безопасность информации. – 1995. – N 3. – С.12-17.

[3] A. Canteaut, M. Trabbia. *Improved fast correlation attacks using parity-check equations of weight 4 and 5, Advances in Cryptology–EUROCRYPT'2000,* Lecture Notes in Computer Science, vol. 1807, Springer-Verlag, 2000 – P. 573–588.

[4] V. Chepyzhov, T. Johansson, B. Smeets, *A simple algorithm for fast correlation attacks on stream ciphers, Fast Software Encryption, FSE'2000,* Lecture Notes in Computer Science, Springer-Verlag, 2000. – P. 313–324.

[5] M. P. C. Fossorier, M. J. Mihaljevic, H. Imai, *Reduced complexity iterative decoding of Low Density Parity Check codes based on Belief Propagation,* IEEE Transactions on Communications, vol. 47, 1999. – P. 673-680.

[6] R. Lidl, H. Niederrieter *Finite fields.* – London: Addison-Wesley Publishing Company, 1983.-819p.

[7] Л. Ковальчук, *Псевдонеприводимые полиномы. Вероятностное тестирование неприводимости* // Кибернетика и системный анализ. – 2004. – №4 – С. 168-176.

[8] О. В. Вербицький, *Вступ до криптології.*/ Львів: Видавництво науково-технічної літератури, 1998. – 247с.

[9] B. Schneier, *Applied cryptography, 2nd Edition, John Wiley & Sons* (1996). [Имеется перевод: Шнайер Б. Прикладная криптография.- М.: "Триумф". – 2002. – 816с., Режим доступу:. http://www.ssl.stu.neva.ru/psw/crypto/html – Заголовок з екрану.].

[10] N. A. Koblitz, *Course of Number Theory and Cryptography.*- Berlin: Springer, 1994.-231p.

[11] Л. В. Скрыпник, Л. В. Ковальчук, *Тест Ферма-Лукаса распознавания полиномов Галуа над кольцами Галуа* // Вісник Східноукраїнського національного університету імені Володимира Даля – 2006. – №2 (103), частина 1. – С. 13-16.

[12] А. А. Нечаев, *Код Кирдока в циклической форме* // Дискретная математика: – 1989. – т.1, вып. 4. – С. 123-139.

[13] А. Н. Алексейчук, А. Л. Волошин, Л. В. Скрыпник, *Совершенная схема множественного разделения секрета на основе линейных преобразований над конечным цепным коммутативным кольцом* // Математика и безопасность информационных технологий. Материалы международной научной конференции по безопасности и противодействия терроризму. Интеллектуальный Центр МГУ. 2 – 3 ноября 2005 г. М.: МЦНМО, 2006. – С. 149 – 154.

[14] H. Pocklington, *The determination of the prime and composite nature of large numbers by Fermat's theorem.* — Proc. Cambridge Phil. Soc, 1914-16, v. 18, p. 29-30.

[15] S. Goldwasser, J. Kilian, *Almost all primes can be quickly certified.* — In: Proceedings of the 18th Annual ACM Symposium on Theory of Computing, 1986, p. 316-329.

[16] R. Schoof, *Elliptic curves over finite fields and the computation of square roots mod p.* — Math. Сотр., 1985, v. 44, p. 483-494.

[17] J. M. Pollard, *Theorems on factorization and primality testing*. — Proc. Cambridge Phil. Soc, 1974, v. 76, p. 521-528.
[18] A. K. Lenstra, H. W. Lenstra, *Jr. Algorithms in number theory*. — Technical Report 87-008. Chicago: University of Chicago, 1987.
[19] H. W. Lenstra, *Jr. Elliptic curves and number-theoretic algorithms*. — Report 86-19. Amsterdam: Mathematisch Instituut, Universiteit van Amsterdam, 1986.
[20] H. W. Lenstra, J*r. Factoring integers with elliptic curves*. — Ann. Math., 1987, v. 126, p. 649-673.

References

[1] М. Глухов. И. Круглов. А. Пичкур, А. Черёмушкин, "Введение в теоретико-числовые методы криптографии" // СПб.: Изд-во "Лань", 2011г., 400с.
[2] Завадская Л. А. Потоковые системы шифрования, основанные на регистрах сдвига. // Безопасность информации. – 1995. – N 3. – С.12-17.
[3] A. Canteaut, M. Trabbia. Improved fast correlation attacks using parity-check equations of weight 4 and 5, Advances in Cryptology– EUROCRYPT'2000, Lecture Notes in Computer Science, vol. 1807, Springer-Verlag, 2000 – P. 573–588.
[4] V. Chepyzhov, T. Johansson, B. Smeets, A simple algorithm for fast correlation attacks on stream ciphers, Fast Software Encryption, FSE'2000, Lecture Notes in Computer Science, Springer-Verlag, 2000. – P. 313–324.
[5] M. P. C. Fossorier, M. J. Mihaljevic, H. Imai. Reduced complexity iterative decoding of Low Density Parity Check codes based on Belief Propagation, IEEE Transactions on Communications, vol. 47, 1999. – P. 673-680.
[6] Lidl R., Niederrieter H. Finite fields. – London: Addison-Wesley Publishing Company, 1983.- 819p.
[7] Ковальчук Л. Псевдонеприводимые полиномы. Вероятностное тестирование неприводимости. // Кибернетика и системный анализ. – 2004. – №4 – С. 168-176.
[8] Вербицький О.В. Вступ до криптології./ Львів: Видавництво науково-технічної літератури, 1998. – 247с.
[9] Schneier B. Applied cryptography, 2nd Edition, John Wiley & Sons (1996). [Имеется перевод: Шнайер Б. Прикладная криптография.- М.: "Триумф". – 2002. – 816с., Режим доступу:. http://www.ssl.stu.neva.ru/psw/crypto/html – Заголовок з екрану.].
[10] Koblitz N. A. Course of Number Theory and Cryptography.- Berlin: Springer, 1994.-231p.
[11] Скрыпник Л.В., Ковальчук Л.В. Тест Ферма-Лукаса распознавания полиномов Галуа над кольцами Галуа // Вісник Східноукраїнського національного університету імені Володимира Даля – 2006. – №2 (103), частина 1. – С. 13-16.
[12] Нечаев А.А. Код Кирдока в циклической форме. // Дискретная математика: – 1989. – т.1, вып. 4. – С. 123-139.
[13] Алексейчук А.Н., Волошин А.Л., Скрыпник Л.В. Совершенная схема множественного разделения секрета на основе линейных преобразований над конечным цепным коммутативным кольцом. // Математика и безопасность информационных технологий. Материалы международной научной конференции по безопасности и противодействия терроризму. Интеллектуальный Центр МГУ. 2 – 3 ноября 2005 г. М.: МЦНМО, 2006. – С. 149 – 154.
[14] Pocklington H. The determination of the prime and composite nature of large numbers by Fermat's theorem. — Proc. Cambridge Phil. Soc, 1914-16, v. 18, p. 29-30.
[15] Goldwasser S., Kilian J. Almost all primes can be quickly certified. — In: Proceedings of the 18th Annual ACM Symposium on Theory of Computing, 1986, p. 316-329.
[16] Schoof R. Elliptic curves over finite fields and the computation of square roots mod p. — Math. Сотр., 1985, v. 44, p. 483-494.
[17] Pollard J. M. Theorems on factorization and primality testing. — Proc. Cambridge Phil. Soc, 1974, v. 76, p. 521-528.
[18] Lenstra A.K., Lenstra H. W.,Jr. Algorithms in number theory. — Technical Report 87-008. Chicago: University of Chicago, 1987.
[19] Lenstra H. W., Jr. Elliptic curves and number-theoretic algorithms. — Report 86-19. Amsterdam: Mathematisch Instituut, Universiteit van Amsterdam, 1986.
[20] Lenstra H. W., Jr. Factoring integers with elliptic curves. — Ann. Math., 1987, v. 126, p. 649-673.

Реферат

Беспалов Олексій

Алгоритми факторизації та перевірки незвідності поліномів з використанням апарату еліптичних кривих

У цій роботі сформульовані та обґрунтовані критерії незвідності поліномів та алгоритми їх факторізації, які є узагальненнями аналогічних критеріїв та алгоритмів для чисел. Особливий цікавим є узагальнення теореми Лєнстра, що забезпечує правильне обчислення кратних точок на еліптичній кривій, які використовуються у алгоритмі Лєнстра. Зазначимо, що доведення узагальнення цієї теореми у випадку поліномів над полем характеристики 2

повністю відрізняється від її доведення у класичному випадку і є дуже нетривіальним.

Використовуючи побудовані критерії, розроблено ряд алгоритмів факторизації та перевірки незвідності поліномів над скінченним полем. Слід зазначити, що основною перевагою даних алгоритмів є не їх швидкодія, а використання в їх структурі абелевих груп, які побудовані на еліптичних кривих. Тому у випадку невдачі можна просто перевибрати еліптичну криву над відповідним полем і повторити алгоритм ще раз. Хоча ці алгоритми і не дають суттєвої переваги у швидкодії, як і їх прообрази – аналогічні алгоритми для чисел, але вони демонструють нові підходи до вирішення давно існуючої та актуальної задачі перевірки незвідності поліномів, а також є досить цікавими з точки зору математики.

Беспалов Алексей

Алгоритмы факторизации и проверки неприводимости полиномов с использованием аппарата эллиптических кривых

В этой работе сформулированы и доказаны критерии неприводимости полиномов и алгоритмы факторизации, которые являются обобщениями аналогичных критериев и алгоритмов для чисел. Особенно интересны является обобщение теоремы Ленстра, которое обеспечивает правильное вычисление кратных точек на эллиптической кривой и используется в алгоритме Ленстра. Заметим, что доказательство обобщения этой теоремы для случая полиномов над полем характеристики 2 полностью отличается от её доказательства в классическом случае и является очень нетривиальным.

Используя построенные критерии, разработан ряд алгоритмов факторизации и проверки неприводимости полиномов над конечным полем. Следует заметить, что основным преимуществом данных алгоритмов является не быстродействие, а использование в их структуре абелевых групп, построенных на эллиптических кривых. Поэтому в случае неудачи можно просто перевыбрать эллиптическую кривую над соответствующим полем и повторить алгоритм ещё раз. Хотя эти алгоритмы и не имеют особого преимущества в быстродействии, як и их прообразы – аналогичные алгоритмы для чисел, но они демонстрируют новые подходы к решениям давно существующей и актуальной задачи проверки неприводимости полиномов, а также являются очень интересными с точки зрения математики.

Bespalov Oleksii

Algorithms for factorization and irreducibility testing of polynomials using elliptic curves

In this article irreducibility criteria and factorization algorithms are formulated and proved, that are generalizations of correspondent criteria and algorithms for integers. Generalization of Lenstra's theorem is of especial interest. It provides correct calculations of multiple points on elliptic curve that is used in Lenstra algorithm. Note that the generalization of this theorem in case of finite field of characteristic 2 is completely different from the classical case and is very non-trivial.

Using the criteria obtained, we construct a series of algorithms for factoring and testing of irreducibility of polynomials over finite field. We should note that their performance isn't their main advantage, but the main advantage is using some abelian group built on elliptic curve. So in case of failure of algorithm we can just chose the other elliptic curve over the corresponding field and repeat the algorithm. These algorithms have no large advantage in speed, like their preimages – analogical algorithms for integers, but they demonstrate new approaches to the solutions of important problem of irreducibility testing and also are very interesting from mathematical point of view.

Відомості про авторів

Беспалов Олексій Юрійович

Освіта: магістр за спеціальністю «Прикладна математика» (2015), Аспірант кафедри ММЗІ КПІ ім. Ігоря Сікорськского.

Область знань: Криптологія, програмування.

Наукові інтереси: Криптографічний захист інформації, прикладна алгебра.

Email: *alexb5dh@gmail.com*

УДК 004.056.5

МЕТОД ВЫЯВЛЕНИЯ РЕЗУЛЬТАТОВ МУЛЬТИ- И ПОЛИКЛОНИРОВАНИЯ В ЦИФРОВОМ ИЗОБРАЖЕНИИ

Кобозева Алла
Одесский национальный политехнический университет

METHOD FOR IDENTIFYING THE RESULTS OF MULTI– AND POLYCLONING IN THE DIGITAL IMAGES

Kobozeva Alla
Odessa National Polytechnic University

Анотація: **Розроблено метод виявлення результатів клонування в цифровому зображенні, заснований на теоретичному базисі, запропонованому автором раніше, ефективний в умовах мульти- (одному прообразу відповідає більше одного клону) і поліклонування (в межах одного зображення задіюється більше одного прообразу) при додаткових, в тому числі значних обурюють впливах на клонована зображення.**
Ключові слова: **Цифрове зображення, клонування, матриця мінімальних блокових відмінностей, постобробка, додаткові впливи.**
Summary: **A method for detecting cloning results in a digital image based on the theoretical basis proposed by the author earlier is developed, effective in multi- (more than one clone corresponds to one prototype) and polycloning (more than one pre-image is involved in one image) with additional ones, including significant ones perturbations on the cloned image.**
Keywords: **Digital image, cloning, matrix of minimal block differences, post processing, additional perturbing effects.**

Введение

При современном уровне развития информационных технологий и компьютерных наук, и сравнительно низкой стоимости современного аппаратного и программного обеспечения возможно легко создавать, изменять и манипулировать цифровыми изображениями (ЦИ). Поэтому чрезвычайно актуален вопрос организации экспертизы целостности ЦИ для возможности их использования с целью, отличной от развлекательной [1].

Одним из наиболее распространенных и часто используемых программных инструментов при неавторизованных изменениях ЦИ является клонирование, реализованное во всех современных графических редакторах (Adobe Photoshop, Gimp и др.), в процессе которого одна область изображения, прообраз копируется и переносится в другую область/области этого же изображения, создавая клон/клоны. На практике для «маскировки» результатов такой операции часто используется постобработка ЦИ, затрудняющая обнаружение клонов и прообраза.

Для выявления результатов клонирования в ЦИ используются три основных подхода: блоково-ориентированный (block-based); основанный на выявлении ключевых точек (key-point based); гибридный. Каждый из перечисленных выше подходов имеет как свои преимущества, так и недостатки [2], [3], [4].

Блоково-ориентированные методы в состоянии достаточно точно локализовать область клона/прообраза. Основным в таких методах является сравнение устанавливаемого количественного признака отличия областей анализируемого ЦИ с пороговым значением, что в общем случае не гарантирует высокую эффективность их использования в условиях анализа ЦИ, не входящих во множество изображений, принимавших участие при определении порога, а также в условиях постобработки с использованием возмущающих воздействий, вид или параметры которых отличны от тех, которые использовались при определении порога.

Алгоритмы, основанные на выявлении ключевых точек, как правило, работают с изображением целиком, не разбивая его на подобласти. Используемые характеристики

относятся ко всему изображению, что в общем случае повышает эффективность вычислений [5]. Двумя основными типами таких методов являются SIFT (Scale Invariant Features Transform) и SURF (Speed UP Robust Features) [6]. Общими основными недостатками таких методов выявления в ЦИ результатов клонирования являются зависимость эффективности методов от размеров областей клона/прообраза, а также от конкретных условий проводимого клонирования. Поскольку основная идея методов данной группы заключается в выделении ключевых точек ЦИ (подобласти ЦИ), эти методы могут оказаться неэффективными в случае, когда клонирование используется с целью удаления некоторого (возможно малого по размерам) объекта с части изображения, которому присущ незначительный перепад значений яркости пикселей. Использование подхода, основанного на анализе ключевых точек, дает меньше возможностей для определения границ областей клона/прообраза, чем использование блоково-ориентированных методов, которые на сегодняшний день остаются более эффективными [3].

В современных разработках, посвященных выявлению результатов клонирования в ЦИ, нашел широкое применение гибридный подход, комбинирующий два или более подходов с целью использования преимущества каждого из них [7]. Чаще всего в тех или иных вариациях используется комбинация block-based и key-point based подходов. Хотя идея использования композиции различных подходов является привлекательной, она не позволяет получить окончательное решение рассматриваемой задачи, устранить ориентированность методов на реализацию конкретных программных средств, используемых при постобработке ЦИ [7].

Поэтому задача выявления результатов клонирования хоть и не является новой, но она остается актуальной. Существующие методы не обеспечивают желаемую эффективность в условиях значительных дополнительных возмущающих воздействий, малых относительных размеров клона в случае, когда клонирование проводится с целью устранения объекта со сцены ЦИ с помощью прообраза, который выбирается из области изображения с малыми перепадами яркости.

В [8] – [9] в рамках блоково-ориентированного подхода предложен новый теоретический базис, основанный на геометрическом представлении изображения, на основе которого разработан метод *KL* выявления результатов клонирования в ЦИ, решающий, благодаря используемому математическому базису, многие из задач, перечисленных выше, эффективный в условиях дополнительных возмущающих воздействий, в том числе значительных, эффективность которого превышает современные аналоги. Однако метод *KL* в общем случае не обеспечивает эффективное выявление результатов мульти- и поликлонирования. При этом мультиклонированием будем называть вариант клонирования, когда одному прообразу отвечает два и более клонов, а поликлонирование – наличие в пределах одного ЦИ двух и более использованных различных прообразов.

Цель статьи и постановка задач

Целью работы является разработка метода выявления результатов клонирования в ЦИ, основанного на теоретическом базисе, разработанном в [8] – [9], эффективного в условиях мульти- и поликлонирования при дополнительных, в том числе значительных, возмущающих воздействиях.

Для достижения поставленной цели в работе необходимо усовершенствовать теоретический базис, разработанный в [8] – [9], для возможности эффективной работы основанного на нем метода в условиях мульти- и поликлонирования при наличии постобработки, в том числе значительной, клонированного изображения. Для этого необходимо: установить характерные особенности матрицы минимальных блоковых отличий, которая ставится в соответствие цифровому изображению, в случае наличия/отсутствия мульти- и поликлонирования; установить характерные особенности гистограмм значений матриц абсолютной разности блоков ЦИ в случае,

когда они принадлежат/не принадлежат областям клонов и прообразов.

Основная часть

Не ограничивая общности рассуждений будем считать, что формальным представлением любого ЦИ является одна $n \times m$ – матрица F с элементами $f_{ij}, i = \overline{1,n},\ j = \overline{1,m}$. Основным объектом анализа при экспертизе ЦИ для выявления результатов клонирования в методе *KL* является $(n-q+1)\times(m-q+1)$ – матрица G минимальных блоковых отличий (ММБО), которая ставится в соответствие ЦИ, где $q \times q$ – размер блока $B_{ij}, i = \overline{1, n-q+1},$ $j = \overline{1, m-q+1}$ матрицы F, для которого на месте (1,1) находится элемент f_{ij} [9].

Каждому блоку B_{ij} ставится в соответствие $(n-q+1)\times(m-q+1)-$матрица блоковых отличий $M^{(ij)}$ с элементами $m^{(i,j)}{}_{k,l} = \sum_{t,p=1}^{q} r_{tp}$, $k = \overline{1, n-q+1}, l = \overline{1, m-q+1}$, где $r_{tp}, t, p = \overline{1,q}$, — элементы $q \times q-$матрицы абсолютной разности блоков ЦИ R, полученной следующим образом:

$$R = \left| B_{ij} - B_{kl} \right|, \qquad (1)$$

где последнее равенство понимается в поэлементном смысле.

Элемент $g_{ij}, i = \overline{1, n-q+1},\ j = \overline{1, m-q+1}$ матрицы G отражает величину наименьшего отличия $q \times q-$блока B_{ij} от любого другого $q \times q-$ блока матрицы F, т.е.

$$g_{ij} = \min M^{(ij)}, i = \overline{1, n-q+1},\ j = \overline{1, m-q+1}. \qquad (2)$$

Для матрицы G в случае единственности клона в [8] – [9] показано, что если B_{ij} и B_{kl} – соответствующие $q \times q-$ блоки, принадлежащие областям клона и прообраза, то выполняется условие

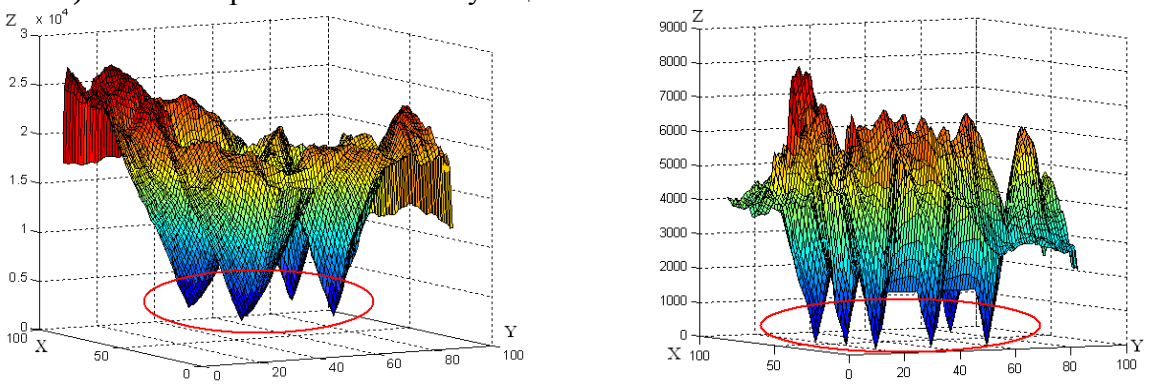
$$g_{ij} = g_{kl}, \qquad (3)$$

где значение $g_{ij} = g_{kl}$ отвечает глобальному (локальному) минимуму G (при этом g_{tp} будем называть глобальным минимумом матрицы G, если $g_{tp} = \min\limits_{i,j} g_{ij}$, и локальным минимумом, если в матрице G существует такая окрестность $U(g_{tp})$ элемента g_{tp}, что для любого элемента матрицы $g_{ij} \in U(g_{tp}), g_{ij} \neq g_{tp}$ имеет место соотношение: $g_{ij} > g_{tp}$). Последнее условие является необходимым условием наличия в ЦИ областей клона и прообраза при наличии/отсутствии постобработки клонированного изображения и основой метода *KL*.

В случае мультиклонирования находит подтверждение гипотеза, выдвинутая ранее в [8] – [9] для единственного клона о том, что одинаковые блоки прообраза и его клонов будут менее других отличаться друг от друга после постобработки ЦИ, т.е. элементы $g_{i_1,j_1}, g_{i_2,j_2}, ..., g_{i_t,j_t}, g_{kl}$ матрицы G, отвечающие блокам $B_{i_1,j_1}, B_{i_2,j_2}, ..., B_{i_t,j_t}$ клонов и соответственно прообраза B_{kl}, будут локальными (глобальными) минимумами G. Однако факт сохранения свойства равенства значений локальных (глобальных) минимумов G может не иметь место для соответствующих блоков прообраза и нескольких клонов в условиях дополнительных возмущающих воздействий (рис. 1.а: прообразу отвечает блок $B_{71,71}$, а клонам – $B_{31,31}, B_{63,31}, B_{31,63}$. Соответствующие элементы G являются ее локальными минимумами, но условие (3) нарушено: $g_{71,71} = 2650,\ g_{31,31} = 2885,\ g_{63,31} = 3076,$ $g_{31,63} = 2650$), оставаясь справедливым в условиях отсутствия постобработки. Действительно, при отсутствии дополнительных возмущающих воздействий соответствующие блоки клонов (независимо от их количества) и прообраза остаются одинаковыми, что приводит к равным по значению соответствующим им глобальным минимумам матрицы G, которые в этом случае нулевые (рис. 1.б: прообразу отвечает блок $B_{80,80}$, клонам – $B_{21,21},\ B_{61,21},\ B_{21,61},$ $B_{41,21},\ B_{21,41}$; соответствующие элементы G

являются ее глобальными минимумами: $g_{80,80} = g_{21,21} = g_{61,21} = g_{21,61} = g_{41,21} = g_{21,41} = 0$).

Процесс постобработки ЦИ в общем случае по-разному (в смысле абсолютного значения) изменит яркость соответствующих пикселей различных клонов, что требует привлечения дополнительных идентификационных признаков матрицы G для их выявления.



а б

Рис. 1 – График функции, интерполирующей элементы матрицы G, отвечающей ЦИ, подвергнутому мультиклонированию: а – с последующим сохранением с потерями (Jpeg с QF=45); б – для клонированного ЦИ без постобработки

В [10] было установлено, что если B_{ij} и B_{kl} – это соответствующие блоки единственного клона и прообраза, то окрестности отвечающих им элементов g_{ij} и g_{kl} матрицы G радиуса $r = 1$ после постобработки будут одинаковыми по значениям соответствующих элементов:

$$g_{i-p,j-q} = g_{k-p,l-q}, \quad p,q \in \{0,1\}, \qquad (4)$$

что не свойственно для блоков оригинальных ЦИ.

В случае мультиклонирования, как уже указывалось выше, различные клоны одного прообраза изменят значения яркости своих соответствующих пикселей в ходе постобработки в общем случае по-разному (хотя эти изменения очевидно будут сравнимыми количественно). Это приведет к нарушению условия (4). Однако, с учетом того, что все области ЦИ обрабатываются после клонирования одинаково, можно предположить, что в окрестностях локальных минимумов G, отвечающих соответствующим блокам клонов и прообраза, будут присутствовать одинаковые по значениям элементы в отличие от большинства оригинальных блоков ЦИ. Практическим подтверждением этому являются результаты вычислительного эксперимента (табл. 1, 2), в котором было задействовано 500 ЦИ в форматах как без потерь, так и с потерями из базы NRCS [11], являющейся традиционной при тестировании алгоритмов, работающих с изображениями. Такое множество ЦИ далее называется экспериментальным множеством (ЭМ).

Таблица 1.

Количество (%) ЦИ из ЭМ, претерпевших мультиклонирование с последующим сохранением с потерями (Jpeg с различными коэффициентами качества QF), для которых окрестности локальных минимумов *G*, отвечающих блокам клонов и прообраза, содержат одинаковые по значению соответствующие элементы

q \ *QF*	25	50	75	90
32	100	100	100	100
24	97	99	100	100
16	95	97	98	99

Таблица 2.

Количество (%) ЦИ из ЭМ, претерпевших мультиклонирование с постобработкой, для которых окрестности локальных минимумов *G*, отвечающих блокам клонов и прообраза, содержат одинаковые по значению соответствующие элементы

q	Тип шума	Параметры шума	Формат сохранения ЦИ после клонирования		(%)
32	Гауссовский	D=0.0001	Tif		100
			Jpeg	QF=85	100
				QF=75	100
				QF=65	100
		D=0.0005	Tif		100
			Jpeg	QF=85	100
				QF=75	100
				QF=65	100
	Мульти-пликативный	D=0.0005	Tif		100
			Jpeg	QF=85	100
				QF=75	100
				QF=65	100
		D=0.001	Tif		100
			Jpeg	QF=85	100
				QF=75	100
				QF=65	99
24	Гауссовский	D=0.0001	Tif		100
			Jpeg	QF=85	100
				QF=75	100
				QF=65	99
		D=0.0005	Tif		100
			Jpeg	QF=85	99
				QF=75	99
				QF=65	97
24	Мульти-пликативный	D=0.0005	Tif		100
			Jpeg	QF=85	99
				QF=75	98
				QF=65	98
		D=0.001	Tif		99
			Jpeg	QF=85	99
				QF=75	98
				QF=65	97
16	Гауссовский	D=0.0001	Tif		98
			Jpeg	QF=85	98
				QF=75	98
				QF=65	98
		D=0.0005	Tif		98
			Jpeg	QF=85	97
				QF=75	97
				QF=65	97
	Мульти-пликативный	D=0.0005	Tif		98
			Jpeg	QF=85	98
				QF=75	97
				QF=65	97
		D=0.001	Tif		97
			Jpeg	QF=85	96
				QF=75	95
				QF=65	94

По результатам анализа полученных результатов установлено, что отрицательным является факт наличия значительного количества ошибок второго рода, когда оригинальные блоки ЦИ трактуются как блоки клона и прообраза. В случае $q=16$ такие блоки возникали практически в каждом ЦИ из ЭМ. Для $q=32$ такие «лже-блоки» появляются редко. Для эффективной работы разрабатываемого метода в случае малых размеров клона и прообраза необходимо привлекать дополнительные качественно/количественные показатели для отделения клона/прообраза от оригинальных областей ЦИ.

Одним из таких дополнительных характерных количественных параметров является показатель возможного отличия между соответствующими $q\times q$ –блоками клона и прообраза, установленный экспериментально в [12]. Привлечение такого показателя T в виде максимально возможного отличия между соответствующими блоками клона и прообраза приводит к значительному сокращению количества ошибок второго рода для разработанного в работе алгоритма. Однако остается возможность для 16*16 блоков появление «лже-блоков». Для сокращения таких случаев по аналогии с [10] исследовались свойства гистограмм матриц R, определяемых в соответствии с формулой (1) для пар блоков ЦИ, принадлежащих/не принадлежащих областям клонов/прообраза (рис. 2, 3).

Установлено, что гистограммы для соответствующих пар блоков из областей клонов и прообраза в случае мультиклонирования имеют характерные особенности по сравнению с гистограммами для пар блоков оригинальных областей ЦИ: максимальное попиксельное отличие в первом случае меньше, чем во втором (количественно установлено: для соответствующих блоков клона и прообраза, соответствующих блоков различных клонов максимальное значение элементов в матрице R, как правило, не превосходят 76); для оригинальных блоков ЦИ часто наблюдался вариант, когда мода гистограммы отличалась от «условного нуля» (соответствующий столбец гистограммы не включал в себя нулевые значения элементов R) (рис. 3), что является нетипичным для блоков клонов и прообраза (рис. 2).

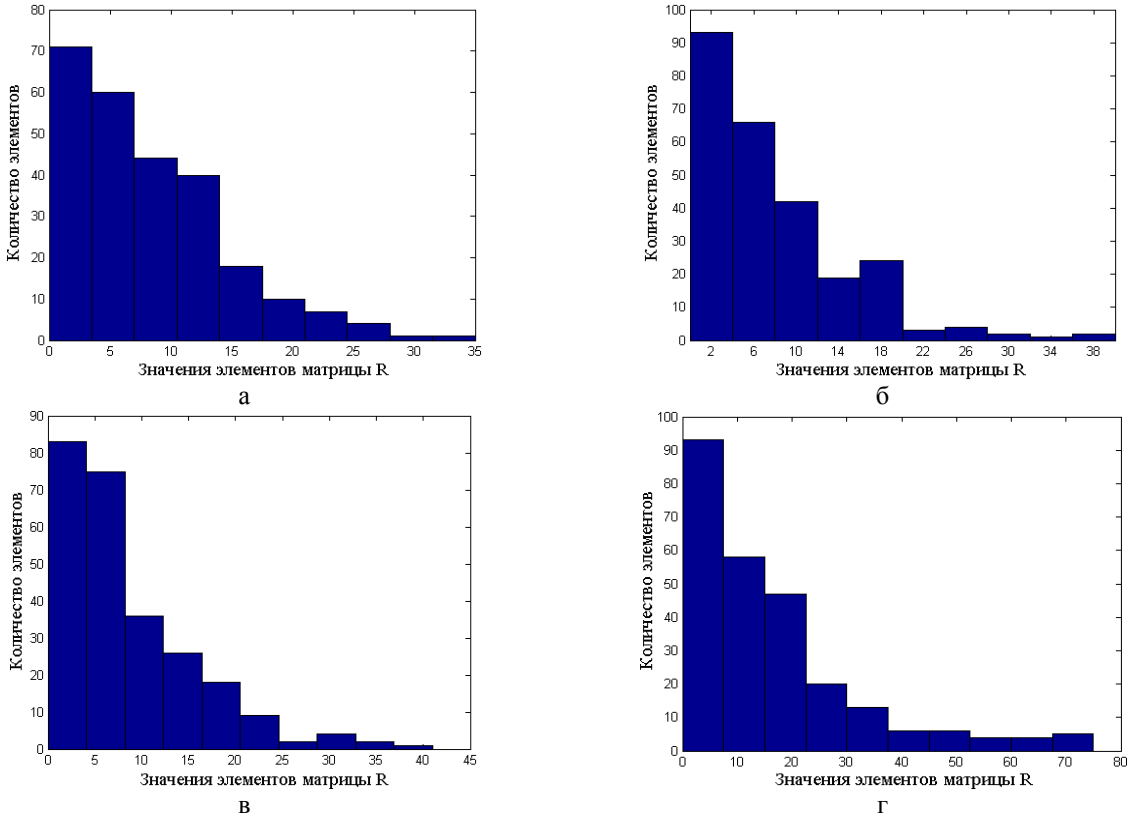


Рис. 2 – Гистограммы элементов матрицы R (блоки 16*16):
а, б, в – пары соответствующих блоков клонов; г – соответствующие блоки клона и прообраза

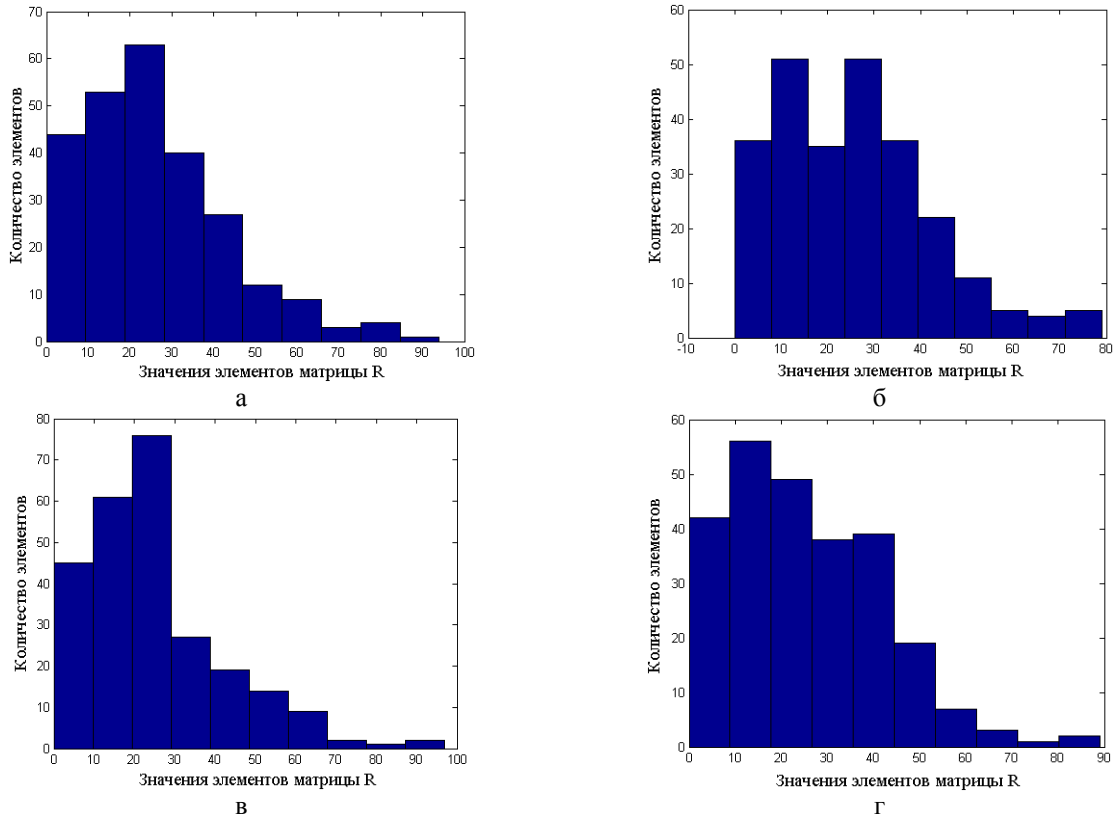


Рис. 3 – Гистограммы элементов матрицы R (блоки 16*16): а, б – оригинальный блок и клон; в - оригинальный блок и прообраз; г – оригинальные блоки, не принадлежащие прообразу

Основные шаги предлагаемого метода выявления результатов мультиклонирования с учетом проведенных исследований выглядят следующим образом:

Шаг 1. Для экспертизы ЦИ с $n \times m -$ матрицей F выбрать размер $q \times q -$ блока.

Шаг 2. В соответствии с (2) построить $(n-q+1)\times(m-q+1)$-ММБО G, отвечающую ЦИ.

Шаг 3. Определить местоположение и значения всех локальных минимумов g_{ij} ММБО G. Для каждого найденного значения g_{ij} проверить:

Если $g_{ij} < T$, где T – установленное пороговое значение для максимального отличия между соответствующими блоками клона и прообраза, то соответствующие локальным минимумам G блоки F являются «подозрительными» на то, чтобы принадлежать областям клонов или прообраза.

Шаг 4. Для всевозможных пар элементов g_{ij} ММБО G, определяющих локальные минимумы G, посчитать количество совпадающих по значению соответствующих элементов матрицы G, находящихся в окрестностях радиуса r локальных минимумов g_{ij}.

Шаг 5. Исключить из «подозрительных» блоки B_{ij}, для которых соответствующие элементы g_{ij} не имеют в своих окрестностях радиуса r совпадающих элементов ни с одной из построенных окрестностей для найденных локальных минимумов G.

Шаг 6. Пусть B_{ij} и B_{kl} - блоки ЦИ такие, что окрестности радиуса r элементов g_{ij} и g_{kl} в матрице G содержат одинаковые по значению соответствующие элементы.

6.1. Построить матрицу $R = \left| B_{i,j} - B_{k,l} \right|$.

6.2. Построить гистограмму значений матрицы R. Для этой гистограммы определить моду t, а также $M = \max_{t,p} r_{tp}$;

если
$(M > 76) OR (t$ *не является* "*условным нулем*"$)$
то пара блоков B_{ij} и B_{kl} не принадлежит областям клона/прообраза,
иначе пара блоков B_{ij} и B_{kl} принадлежит областям клона/прообраза. Эти блоки отмечаются соответствующим образом на анализируемом ЦИ (например, закрашиваются в одинаковый цвет).

Иллюстрация работы алгоритмической реализации предложенного метода в случае $q = 24$, T=10500, $r = 2$ в условиях значительных дополнительных возмущающих воздействий представлена на рис. 4.

а б в

Рис. 4 – Результаты выявление мультиклонирования разработанным методом:
а – исходное ЦИ; б – результат мультиклонирования с последующим наложением гауссовского шума (SNR=4.7dB) и сохранения в Jpeg с QF=75; в – результат выявления областей клонов и прообраза (блоки, отвечающие выявленным областях, окрашены в белый цвет)

Принципиально ничего не изменится в работе метода, если операция клонирования будет проведена не для одного, а для нескольких прообразов в пределах одного ЦИ. Дополнительной задачей здесь является задача разделения групп «прообраз - его клоны», отвечающих различным прообразам. Решение этой задачи предлагается осуществлять при помощи анализа графа, формируемого следующим образом. Найденным в ходе выполнения шагов 1-6 предложенного выше метода блокам B_{ij}, принадлежащим областям клонов и прообразов, ставится в соответствие неориентированный граф $E(V, X)$ с множеством вершин V и множеством ребер X по следующему правилу: каждому найденному блоку B_{ij} отвечает вершина графа с некоторой меткой, например, (i, j); вершины графа (i, j) и (k, l) смежны, т.е. образуют ребро, тогда и только тогда, когда окрестности элементов g_{ij} и g_{kl} имеют одинаковые по значению соответствующие элементы в матрице G.

Для выявления поликлонирования в ЦИ предложенный выше метод усовершенствуется путем добавления следующих шагов.

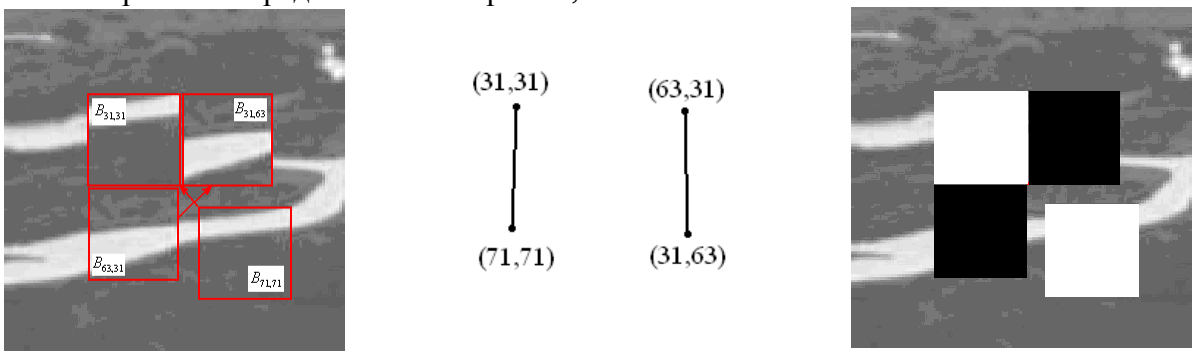
Шаг 7. Построить граф $E(V, X)$.

Шаг 8. Определить $\bar{k}$ – количество компонент связности графа $E(V, X)$.

Если $\bar{k} = 1$,
то поликлонирование отсутствует; при клонировании использовался один прообраз;
иначе поликлонирование имело место, при клонировании использовалось $\bar{k}$ прообразов. Блоки, соответствующие вершинам, попавшим в одну компоненту

связности графа $E(V,X)$, образуют группу «прообраз - его клоны».

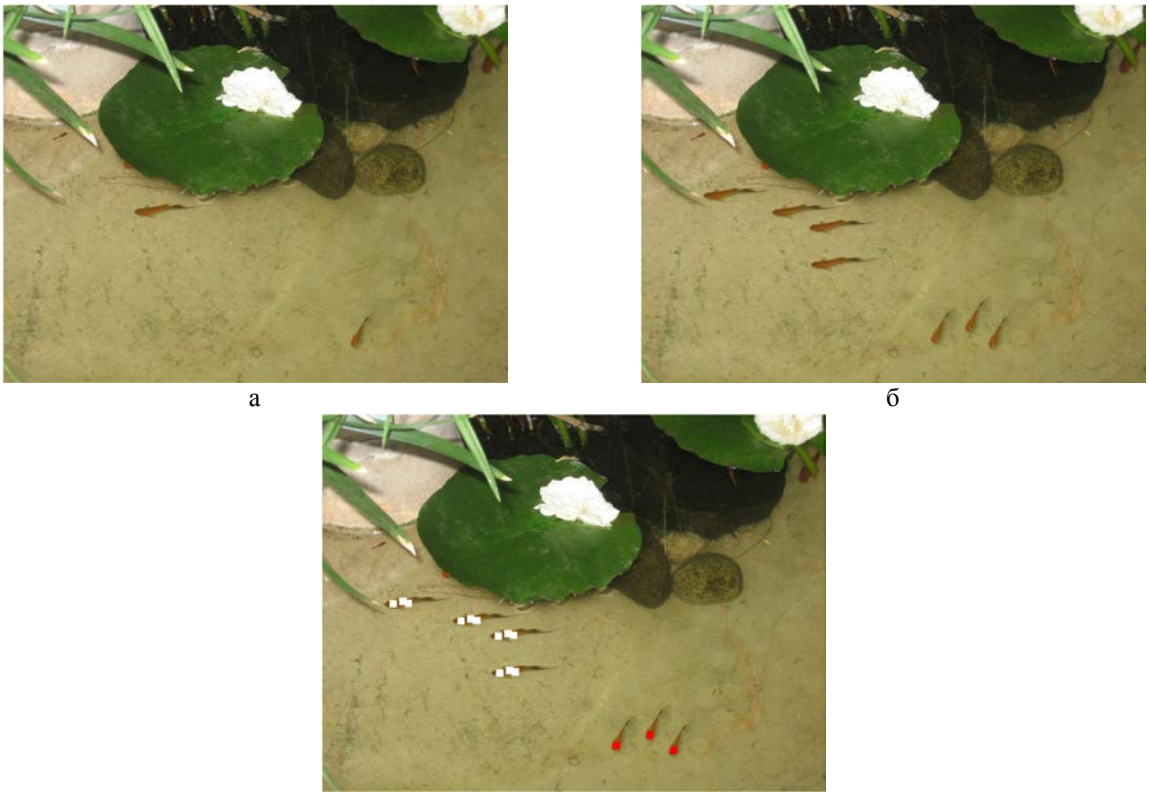
Иллюстрация работы предложенного метода на стадии выявления результатов поликлонирования представлена на рис. 5, где каждая из двух компонент связности полученного графа $E(V,X)$ отвечает отдельной группе «прообраз - клон», что соответствует действительности.



а б в

Рис. 5 – Выявление результатов поликлонирования разработанным методом: а – результат поликлонирования ЦИ с последующим сохранением в формат с потерями; б – граф $E(V,X)$; в – результат выявления клонирования (разные группы «прообраз-его клон» выделены разными цветами)

Результаты работы разработанного метода при выявлении поли- и мультиклонирования в условиях постобработки клонированного ЦИ представлены на рис. 6.



а б в

Рис. 6 – Результаты выявления поли- и мультиклонирования разработанным методом: а – исходное ЦИ; б - результат поли- и мультиклонирования в условиях сохранения ЦИ с потерями (формат Jpeg с коэффициентом качества QF=65); в – результат работы метода (разные группы «прообраз - его клоны» выделены разными цветами)

Таким образом, разработанный метод позволяет в условиях дополнительных возмущающих воздействий выявлять результаты мультиклонирования, в том числе при наличии нескольких прообразов, разделяя группы «прообраз – его клоны».

Выводы

В работе разработан метод выявления результатов клонирования в цифровом изображении в условиях его постобработки на основе дальнейшего развития теоретического базиса для организации процесса выявления нарушений целостности изображения, предложенного автором ранее. Основным объектом анализа является матрица G минимальных блоковых отличий, которая ставится в соответствие изображению, подвергаемому экспертизе. В ходе развития теоретического базиса установлено обязательное наличие совпадающих по значению соответствующих элементов в окрестностях локальных/глобальных минимумов матрицы G, отвечающих блокам прообраза/клонов, в том числе в условиях неединственности клона и прообраза. Об этом свидетельствуют характерные особенности гистограмм значений элементов матрицы абсолютной разности блоков ЦИ в случаях их принадлежности/непринадлежности клонам/прообразам. Результаты проведенных вычислительных экспериментов свидетельствуют, что разработанный метод является эффективным в случаях мульти- и поликлонирования.

Перелік посилань

[1] N. P. Jogl ekar, *A Compressive Survey on Active and Passive Methods for Image Forgery Detection* / N. P. Joglekar, P. N. Chatur // International Journal of Engineering and Computer Science. – 2015. – Vol. 4, Iss. 1. – Pp. 10187–10190.

[2] Ratnam Singh, *Copy Move Tampering Detection Techniques: A Review* / Ratnam Singh, Mandeep Kaur //International Journal of Applied Engineering Research. – 2016. – Vol. 11, No 5. – Pp. 3610–3615.

[3] S. Rani, *A Survey of Copy-Move Forgery Detection Techniques for Digital Images* / S. Rani, M. Jayamohan, S. Sruthy // International Journal of Innovations in Engineering and Technology. – 2015. – Vol.5, Iss.2. – Pp.419–426.

[4] Sawinder Singh Mangat. *A review of literature on copy-move forgery detection techniques* / Sawinder Singh Mangat, Harpreet Kaur // International Journal of Computer Science and Information Technology & Security (IJCSITS). – 2016. – Vol.6, No 1. – P.482–486.

[5] Harpreet Kaur. *Key-point based copy-move forgery detection and their hybrid methods: A Review/ Harpreet Kaur, Jyoti Saxena, Sukhjinder Singh //* Journal of The International Association of Advanced Technology and Science. – 2015. - Vol. 16, No 02. Режим доступа: http://www.jiaats.com/Journals-Pdf/June-2015/Jeee/Jeee-2.pdf.

[6] Yu Liyang. *Feature Point-based Copy-Move Forgery Detection: Covering the Non-Textured Areas/* Yu Liyang, Han Qi, Niu Xiamu // International Journal of Multimedia Tools and Applications,Springer. – 2015. - Vol. 74, Iss. 4. - Pp. 1-18.

[7] Diaa M. Uliyan. *Image Region Duplication Forgery Detection Based on Angular Radial Partitioning and Harris Key-Points* / Diaa M. Uliyan, Hamid A. Jalab, Ainuddin W. Abdul Wahab, Somayeh Sadeghi // Symmetry. – 2016. – Vol. 8, Iss. 7. – Pp. 56–65.

[8] А. А. Кобозева, *Основы нового подхода к выявлению результатов клонирования в цифровом изображении в условиях возмущающих воздействий* / А. А. Кобозева, С .Н. Григоренко // Інформатика та математичні методи в моделюванні. – 2015. – Т.5, №4. – С.303–311.

[9] A. A. Kobozeva, *New approach development for solution of cloning results detection problem in lossy saved digital image* / A. A. Kobozeva, S. M. Grigorenko // Odes'kyi Politechnichnyi Universytet. Pratsi. – 2016. – Iss. 2. - PP. 62–69.

[10] С. Н. Григоренко, *Усовершенствование метода обнаружения результатов фальсификации в цифровом изображении в условиях атак* / А. А. Кобозева, С. Н. Григоренко // Проблемы региональной энергетики. Электронный журнал Академии наук Республики Молдова. – 2016. – №2 (31). – С. 93–103.

[11] *NRCS Photo Gallery: [Електронний ресурс] //* United States Department of Agriculture. Washington, USA. Режим доступа: http://photogallery.nrcs.usda.gov.

[12] С. М. Григоренко, *Розвиток методу виявлення клонування в цифровому зображенні в умовах додаткових збурних дій* / С. М. Григоренко // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2016. – Вип. 1(31). – С. 85–98.

References

[1] N. P. Jogl ekar, *A Compressive Survey on Active and Passive Methods for Image Forgery Detection* / N. P. Joglekar, P. N. Chatur // International Journal of Engineering and Computer Science. – 2015. – Vol. 4, Iss. 1. – Pp. 10187–10190.

[2] Ratnam Singh, *Copy Move Tampering Detection Techniques: A Review* / Ratnam Singh, Mandeep Kaur //International Journal of Applied Engineering Research. – 2016. – Vol. 11, No 5. – Pp. 3610–3615.

[3] S. Rani, *A Survey of Copy-Move Forgery Detection Techniques for Digital Images* / S. Rani, M. Jayamohan, S. Sruthy // International Journal of Innovations in Engineering and Technology. – 2015. – Vol.5, Iss.2. – Pp.419–426.

[4] Sawinder Singh Mangat. *A review of literature on copy-move forgery detection techniques* / Sawinder Singh Mangat, Harpreet Kaur // International Journal of Computer Science and Information Technology & Security (IJCSITS). – 2016. – Vol.6, No 1. – P.482–486.

[5] Harpreet Kaur. *Key-point based copy-move forgery detection and their hybrid methods: A Review/ Harpreet Kaur, Jyoti Saxena, Sukhjinder Singh //* Journal of The International Association of Advanced Technology and Science. – 2015. - Vol. 16, No 02. Режим доступа: http://www.jiaats.com/Journals-Pdf/June-2015/Jeee/Jeee-2.pdf.

[6] Yu Liyang. *Feature Point-based Copy-Move Forgery Detection: Covering the Non-Textured Areas/* Yu Liyang, Han Qi, Niu Xiamu // International Journal of Multimedia Tools and Applications,Springer. – 2015. - Vol. 74, Iss. 4. - Pp. 1-18.

[7] Diaa M. Uliyan. *Image Region Duplication Forgery Detection Based on Angular Radial Partitioning and Harris Key-Points* / Diaa M. Uliyan, Hamid A. Jalab, Ainuddin W. Abdul Wahab, Somayeh Sadeghi // Symmetry. – 2016. – Vol. 8, Iss. 7. – Pp. 56–65.

[8] A. A. Kobozeva, *Osnovы novogo podxoda k vыyavleny`yu rezul`tatov klony`rovany`ya v cy`frovom y`zobrazheny`y` v uslovy`yax vozmushhayushhy`x vozdejstvy`j* / A. A. Kobozeva, S .N. Gry`gorenko // Informaty`ka ta matematy`chni metody` v modelyuvanni. – 2015. – T.5, #4. – S.303–311.

[9] A. A. Kobozeva, *New approach development for solution of cloning results detection problem in lossy saved digital image* / A. A. Kobozeva, S. M. Grigorenko // Odes'kyi Politechnichnyi Universytet. Pratsi. – 2016. – Iss. 2. - PP. 62–69.

[10] S. N. Gry`gorenko, *Usovershenstvovany`e metoda obnaruzheny`ya rezul`tatov fal`sy`fy`kacy`y` v cy`frovom y`zobrazheny`y` v uslovy`yax atak* / A. A. Kobozeva, S. N. Gry`gorenko // Problemы regy`onal`noj эnergety`ky`. Эlektron¬nыj zhurnal Akademy`y` nauk Respubly`ky` Moldova. – 2016. – #2 (31). – S. 93–103.

[11] *NRCS Photo Gallery: [Електронний ресурс] //* United States Department of Agriculture. Washington, USA. Rezhym dostupa: http://photogallery.nrcs.usda.gov.

[12] С. М. Gry`gorenko, Rozvy`tok metodu vy`yavlennya klonuvannya v cy`frovomu zobrazhenni v umovax dodatkovy`x zburny`x dij / S. M. Gry`gorenko // Pravove, normaty`vne ta metrologichne zabezpechennya sy`stemy` zaxy`stu informaciyi v Ukrayini. – 2016. – Vy`p. 1(31). – S. 85–98.

Реферат

Кобозєва Алла

Метод виявлення результатів мульти- і поліклонування в цифровому зображенні

Сучасний рівень розвитку інформаційних технологій і комп'ютерних наук дозволяє легко створювати, змінювати і маніпулювати цифровими зображеннями, що робить надзвичайно актуальним питання організації експертизи їх цілісності.

Одним з найбільш поширених і часто використовуваних програмних інструментів при неавторизованих змінах зображення є клонування, при проведенні якого на практиці для його «маскування» використовується постобробка зображення, що ускладнює виявлення клонів і прообразу.

Існуючі методи не забезпечують бажану ефективність в умовах значних додаткових збурних дій, малих відносних розмірів клону в разі, коли клонування проводиться з метою усунення об'єкта зі сцени зображення за допомогою прообразу, який вибирається з області з малими перепадами яскравості.

Автором в рамках блоково-орієнтованого підходу розроблено метод KL виявлення результатів клонування в цифровому зображенні, ефективність якого перевищує ефективність сучасних аналогів.

Робота присвячена розробці методу виявлення результатів клонування в зображенні, ефективного в умовах мульти- і поліклонування при додаткових, в тому числі значних збурних діях, шляхом подальшого розвитку теоретичного базису. Основним об'єктом аналізу при експертизі цифрового зображення, формальним представленням якого є $n \times m -$ матриця F з елементами $f_{ij}, i = \overline{1,n},\ j = \overline{1,m}$, виступає $(n-q+1)\times(m-q+1)$-матриця G мінімальних блокових відмінностей, яка ставиться у відповідність зображенню після попереднього вибору розміру $q \times q -$ блоку, сукупність яких визначає покриття F. Елемент $g_{ij}, i = \overline{1,n-q+1},\ j = \overline{1,m-q+1}$, матриці G відображає величину найменшої відмінності $q \times q -$ блоку B_{ij}, що відповідає елементу f_{ij}, від будь-якого іншого $q \times q -$ блоку матриці F. Якщо B_{ij} і B_{kl} - це відповідні блоки єдиного клону і прообразу, то околи радиуса $r = 1$ локальних мінімумів g_{ij} і g_{kl} матриці G, які їм відповідають, після постобробки будуть однаковими за значеннями відповідних елементів: $g_{i-p,\,j-q} = g_{k-p,\,l-q},\ \ p, q \in \{0,1\}$, що не властиво для блоків оригінальних ЦЗ. У разі мультіклонування встановлено, що в околах локальних мінімумів G, що відповідають блокам клонів і прообразу, будуть присутні однакові за значеннями елементи, на відміну від більшості оригінальних блоків ЦЗ. Гістограми значень елементів матриці $R = \left| B_{ij} - B_{kl} \right|$ для відповідних пар блоків B_{ij}, B_{kl} з областей клонів і прообразу в разі мультиклонування має характерні особливості в порівнянні з гістограмами для пар блоків оригінальних областей ЦЗ: максимальна попіксельна відміна в першому випадку менша, ніж у другому; для оригінальних блоків ЦЗ мода гістограми, як правило, відрізняється від «умовного нуля» (відповідний стовпець гістограми не включає в себе нульові значення елементів R).

Врахування виявлених особливостей околів локальних (глобальних) мінімумів матриці G і гістограм значень R дозволяє визначити відповідні блоки клонів і прообразів. Для вирішення цієї задачі слід здійснювати аналіз графа, який формується наступним чином. Знайденим блокам B_{ij}, що належать областям клонів і прообразів, ставиться у відповідність неорієнтований граф $E(V, X)$ з множиною вершин V і множиною ребер X за наступним правилом: кожному блоку B_{ij} відповідає вершина графа з міткою (i, j); вершини графа (i, j) і (k, l) є суміжними, тобто утворюють ребро, тоді й тільки тоді, коли околи елементів g_{ij} і g_{kl} однакового радіусу мають однакові за значенням відповідні елементи в матриці G. Кількість компонент зв'язності графа $E(V, X)$ визначає кількість різних прообразів, що були використані в процесі поліклонування, а блоки, для яких відповідні вершини потрапили в одну компоненту зв'язності графа $E(V, X)$, утворюють групу «прообраз - його клони».

Кобозева Алла

Метод выявления результатов мульти- и поликлонирования в цифровом изображении

Современный уровень развития информационных технологий и компьютерных наук позволяет легко создавать, изменять и манипулировать цифровыми изображениями, что делает чрезвычайно актуальным вопрос организации экспертизы их целостности.

Одним из наиболее распространенных и часто используемых программных

инструментов при неавторизованных изменениях изображения является клонирование, при проведении которого на практике для его «маскировки» используется постобработка изображения, затрудняющая обнаружение клонов и прообраза.

Существующие методы не обеспечивают желаемую эффективность в условиях значительных дополнительных возмущающих воздействий, малых относительных размеров клона в случае, когда клонирование проводится с целью устранения объекта со сцены изображения с помощью прообраза, который выбирается из области с малыми перепадами яркости.

Автором в рамках блоково-ориентированного подхода разработан метод *KL* выявления результатов клонирования в цифровом изображении, эффективность которого превышает эффективность современных аналогов.

Работа посвящена разработке метода выявления результатов клонирования в изображении, эффективного в условиях мульти- и поликлонирования при дополнительных, в том числе значительных возмущающих воздействиях, путем дальнейшего развития теоретического базиса. Основным объектом анализа при экспертизе цифрового изображения, формальным представлением которого является $n \times m -$матрица F с элементами $f_{ij}, i = \overline{1,n},\ j = \overline{1,m}$, служит $(n-q+1)\times(m-q+1)$-матрица G минимальных блоковых отличий, которая ставится в соответствие изображению после предварительного выбора размера $q \times q -$блока, совокупность которых определяет покрытие F. Элемент $g_{ij}, i = \overline{1,n-q+1},\ j = \overline{1,m-q+1}$, матрицы G отражает величину наименьшего отличия $q \times q -$блока B_{ij}, отвечающего элементу f_{ij}, от любого другого $q \times q -$блока матрицы F. Если B_{ij} и B_{kl} - это соответствующие блоки единственного клона и прообраза, то окрестности отвечающих им локальных минимумов g_{ij} и g_{kl} матрицы G радиуса $r = 1$ после постобработки будут одинаковыми по значениям соответствующих элементов: $g_{i-p,j-q} = g_{k-p,l-q},\ p,q \in \{0,1\}$, что не свойственно для блоков оригинальных ЦИ. В случае мультиклонирования установлено, что в окрестностях локальных минимумов G, отвечающих соответствующим блокам клонов и прообраза будут присутствовать одинаковые по значениям элементы, в отличие от большинства оригинальных блоков ЦИ. Гистограммы значений элементов матрицы $R = |B_{ij} - B_{kl}|$ для соответствующих пар блоков B_{ij}, B_{kl} из областей клонов и прообраза в случае мультиклонирования имеет характерные особенности по сравнению с гистограммами для пар блоков оригинальных областей ЦИ: максимальное попиксельное отличие в первом случае меньше, чем во втором; для оригинальных блоков ЦИ мода гистограммы, как правило, отличается от «условного нуля» (соответствующий столбец гистограммы не включает в себя нулевые значения элементов R).

Учет выявленных особенностей окрестностей локальных (глобальных) минимумов матрицы G и гистограмм значений R позволяет определить соответствующие блоки клонов и прообразов. Для решение этой задачи предлагается осуществлять анализ графа, формируемого следующим образом. Найденным блокам B_{ij}, принадлежащим областям клонов и прообразов, ставится в соответствие неориентированный граф $E(V, X)$ с множеством вершин V и множеством ребер X по следующему правилу: каждому блоку B_{ij} отвечает вершина графа с меткой (i, j); вершины графа (i, j) и (k, l) смежны, т.е. образуют ребро, тогда и только тогда, когда окрестности элементов g_{ij} и g_{kl} одинакового радиуса имеют одинаковые по значению соответствующие элементы в матрице G. Количество компонент

связности графа $E(V, X)$ определяет количество различных прообразов, использованных в процессе поликлонирования, а блоки, для которых соответствующие вершины попали в одну компоненту связности графа $E(V, X)$, образуют группу «прообраз - его клоны».

Kobozeva Alla

Method for identifying the results of multi– and polycloning in the digital images

The modern level of development of information technology and computer science makes it easy to create, modify and manipulate of the digital images, which makes the issue of organization of expertise of their integrity is extremely urgent. One of the most common and frequently used software tools for unauthorized image changes is cloning, which in practice uses a post-processing image to hide it, making it difficult to detect clones and their pre-images.

The efficiency of proposed method exceeds the efficiency of modern analogues.

The aim of the research is development of a method for identifying the results of cloning in the digital images that is effective under multi– and polycloning conditions with additional significant perturbations.

The main analyzed object during in the examination of a digital image, the formal representation of which is n×m-matrix with elements, is (n–q+1)(m–q+1)-matrix of minimal block differences that is matched to the image after a preliminary choice of q×q-block size, the plurality of which determines the overlapping. The element of matrix determines the magnitude Bij of the smallest difference of q×q-block, which corresponded to element , from any other q×q-block of the matrix.

It is established that in the case of multicloning in the vicinity of local minima which responsible to the corresponding blocks of clones and the pre-image, the elements identical in values will be present, unlike most original blocks of the digital image.

It is established that the histograms of the values of the matrix elements for the corresponding pairs of blocks from the clone and pre-image regions in the case of multicloning have characteristic features compared to histograms for pairs of blocks of original digital image’s regions: the maximum per-pixel difference in the first case is smaller than in the second; for the original digital image’s blocks the histogram mode is usually different from the "conditional zero" (the corresponding histogram column does not include zero elements R).

The allowance for the revealed features of the neighborhoods of the local (global) minima of the matrix G and the histograms of the values R, it is possible to determine the corresponding blocks of clones and pre-images. The solution of this problem is proposed to be carried out by means of an analysis of the graph formed as follows. The blocks Bij, that belong to the domains of clones and pre-images, are associated with an unoriented graph E(V, X) with a set of vertices V and a set of edges X according to the following rule: each block Bij has a vertex with a label (i, j); the vertices (i, j) and (k, l) of the graph are adjacent, i.e. they form an edge if and only if the neighborhoods of elements gij and gkl of the same radius have the same value in the relevant elements in the matrix G. The number of connected components of the graph E(V, X) determines the number of different pre-images used in the polycloning process, and the blocks, for which the corresponding vertices fall into one connected component of the graph E(V, X), form the group “pre-image - its clones”.

Відомості про автора

Кобозєва Алла Анатоліївна

Освіта: Вища, прикладна математика (1988).

Науковий ступінь: Доктор технічних наук (2009).

Вчене звання: Професор.

Місце роботи: Одеський національний політехнічний університет.

Область знань: Системи захисту інформації.

Наукові інтереси: Стеганографія, методи перевірки та забезпечення цілісності цифрових контентів, обчислювальні методи, матричний аналіз, теорія збурень.

Email: *Alla_kobozeva@ukr.net*

4. Технічні засоби системи захисту інформації. Визначення відповідності засобів ТЗІ

УДК 621.37:621.391

СООТНОШЕНИЯ УРОВНЕЙ ГАРМОНИК РАССЕЯНОГО ПОЛЯ В НЕЛИНЕЙНОЙ ЛОКАЦИИ

Зинченко Максим[1]; Во Зуй Фук[1]; Зиньковский Юрий[1]; Прокофьев Михаил[2]
[1]КПІ ім. Ігоря Сікорського;
[2]НДЦ «ТЕЗІС» КПІ ім. Ігоря Сікорського

THE RATIO OF THE HARMONICS LEVELS OF THE SCATTERED FIELD IN NONLINEAR LOCATIONS

Zinchenko Maksym[1]; Vo Duy Phuc[1]; Zinkovskiy Yuriy; Prokofiev Mikhail[2]
[1]Igor Sikorsky Kyiv Polytechnic Institute;
[2]SRC «TESIS» Igor Sikorsky Kyiv Polytechnic Institute

Анотація: **Показано, що пошук радіоелектронної апаратури як нелінійних розсіювачів (НРС) раціонально здійснювати детектором нелінійних переходів (NLJD - Non Linear Junction Detector). Ефективність використання NLJD пов'язана з вибором порогових значень співвідношення рівнів прийнятих кратних гармонік. Аналітично досліджено, що завищення граничного значення демаскуючої ознаки доцільно лише для "потужних" випромінювань NLJD при зондуванні НРС з "малою" нелінійною ефективною площею розсіювання (НЕПР). Поріг, як критерій достовірної ідентифікації, неефективний для "малопотужних" випромінювань NLJD при зондуванні НРС з "великою" НЕПР.**
Ключові слова: **Детектор нелінійних переходів, нелінійний розсіювач, імітатор закладного пристрою.**
Summary: **This article is shown that the search for radio-electronic equipment as a nonlinear scatters (NS) efficiently carries out the Non Linear Junction Detector (NLJD). The efficiency of using NLJD is related tothe choice of the threshold values of the ratios of the levels received multiple harmonics. Analytically investigated that overestimation of the threshold of the unmasking feature is only appropriate for “strong” radiation of NLJD in probing NS with small non-linear effective square of scatterer. The threshold as a criterion of reliable identification of is not effective for the “low power” radiation NLJD in probing NS with “big” non-linear effective square of scatterer.**
Keywords: **Non linear junction detector, nonlinear scatters, electronic device simulator.**

Введение

Нелинейная радиолокация широко используется для обнаружения закладных устройств (ЗУ) с радиоэлектронной элементной базой. К ЗУ относятся устройства несанкционированного доступа к информации, дистанционно управляемые электроникой взрывоопасные предметы, идентификационные радиомаркеры и др. Поиск ЗУ методами нелинейной радиолокации осуществляется с помощью детекторов нелинейных переходов (NLJD – Non Linear Junction Detector). Преимущество детектора нелинейных переходов в сравнении с детектором поля и анализатором спектра состоит в возможности выявлять ЗУ, которые не излучают демаскирующие электромагнитные поля [1], [2]. Любое ЗУ является нелинейным рассеивателем (НРс) с эквивалентной антенной структурой и нелинейными нагрузками в виде полупроводниковых элементов. При зондировании НРс моногармоническим или импульсным СВЧ сигналом в пространство излучаются в результате нелинейных преобразований (НП) сигналы отклика

(СО), например, кратные гармоники. Во время работы с NLJD выявление "значимых" по уровню НП свидетельствует о наличии ЗУ в исследуемом пространстве. Места проведения поиска ЗУ могут иметь также структуры коррозионного происхождения типа "металл-окисел-металл" (МОМ-структуры). Попавшие под зондирование МОМ-структуры также излучают НП в спектре СО, что создает определенные трудности в процессе выявления ЗУ. Большее распространение приобрели NLJD, которые принимают вторую и третью гармоники частоты зондирующего сигнала (ЗС) [1]. Различение искомых НРс на фоне МОМ-структур осуществляется по соотношению уровней мощности принятых гармоник. Для ЗУ уровень второй гармоники превышает уровень третьей на 20–40 дБ. При зондировании МОМ-структур излучается третья гармоника, а уровень второй гармоники, как правило, соизмерим с уровнем шума. Разное соотношение уровней принятых гармоник связано с формой вольт-амперных характеристик (ВАХ) нелинейных объектов. Полупроводниковым элементам в составе ЗУ соответствуют несимметричные ВАХ, рассеивающим МОМ-структурам – симметричные [1].

По уровню мощности ЗС детекторы нелинейных переходов условно делят на "мощные" и "маломощные". Импульсные NLJD (выходная мощность 100–600 Вт в импульсе, частота следования импульсов $400–100\cdot10^3$ Гц при скважности 100–1000), как правило, считаются "мощными". Детекторы нелинейных переходов непрерывного действия (выходная мощность до 1,5 Вт) относят к "маломощным". Динамический диапазон приёмников NLJD не меньше 40 дБ, а их чувствительность не хуже -80 (-130) дБ/Вт (при соотношении сигнал/шум 6 дБ). У импульсных NLJD чувствительность приемников на три порядка меньше чем в NLJD непрерывного действия. Соотношение сигнал/шум на входе приемника импульсного NLJD примерно на три порядка больше чем у локатора непрерывного действия. Коэффициент усиления передающей антенны NLJD не менее 6 дБ, а приёмной – не менее 8 дБ. Поляризация антенн круговая, коэффициент эллиптичности не хуже 0,8. Уровень заднего лепестка диаграммы направленности (ДН) передающей и приёмной антенн не больше -15 дБ [1].

Типичное ЗУ имеет сложную эквивалентную антенную структуру с несистематизированной топологией. Качественно такая "случайная" антенна есть ансамблем диполей разной длины и ориентации. Элементарными диполями выступают выводы радиоэлектронных приборов, дорожки печатных плат, металлизированные поверхности и т.д. По отношению к длине волны ЗС NLJD антенные структуры ЗУ делятся на "электрически малые" (меньше на порядок и более длины волны ЗС) и "электрически соизмеримые". Соответственно "электрически малым" антенным структурам свойственна малая нелинейная эффективная площадь рассеивания (НЭПР) зондирующего сигнала. Поэтому НРс с "малой" НЭПР характеризуются "слабым излучением" НП при зондировании. Рассеиватели с "электрически соизмеримыми" антенными структурами имеют достаточно "большую" НЭПР и переизлучают достаточно мощный СО.

Постановка задачи

Увеличение плотности потока мощности ЗС может привести к деформации ВАХ полупроводниковых элементов ЗУ (с возможным последующим электрическим или тепловым пробоем). Деформации ВАХ полупроводниковых элементов ЗУ во время зондирования приводят к изменению уровней излученных нелинейных продуктов. Здесь немаловажную роль играет индуктивный разогрев рассеивателя как диэлектрической среды с различными проводящими включениями. Например, при зондировании симметричного вибратора с диодом в нагрузке деформация ВАХ полупроводникового прибора

возникает из-за эффекта разогрева свободных носителей заряда в СВЧ поле [3], [4]. Явление диссипации приводит к нарушению равновесного состояния полупроводниковой структуры из-за ее разогрева на температуру ΔT. Тепловую восприимчивость полупроводникового прибора в составе ЗУ к уровню воздействующего ЗС определим выражением $Z = \frac{(T_0 + \Delta T)/T_0}{(P_0 + \Delta P)/P_0}$, где T_0 – температура при нормальных условиях, P_0 – максимальный уровень воздействующей на НРс мощности ЗС NLJD, не приводящий к деформации ВАХ, ΔP – прирост уровня мощности ЗС NLJD. Введем понятие коэффициента устойчивости полупроводникового прибора на действие определённого уровня мощности ЗС NLJD γ, $\gamma = T_0/(T_0 + \Delta T)$, $\gamma_{\max} = 1$, $\gamma_{\min}$ ограничена пробоем.

Повышение эффективности использования NLJD также предполагает задание пороговых уровней на минимальные уровни принятых кратных гармоник Q_i и их соотношения $L_{i,j}$ (i, j – номера гармоник, $i, j = 2, 3, \ldots$, $i \neq j$). Для большинства NLJD значимым есть пороговое соотношение уровней $L_{2,3}$ (далее просто L). Величина L может служить критерием верной идентификации НРс, особенно при зондировании среды “маломощными” NLJD. Выбор значения L требует рационального удовлетворения двум противоречивым правилам. Чем больше L, тем выше эффективность обнаружения и идентификации ЗУ. С увеличением L также возрастает вероятность пропуска ЗУ. Актуальным становится аналитическая оценка оптимальных значений L с учетом уровня действующей мощности ЗС NLJD и НЭПР закладного устройства.

Основная часть

В экспериментах по определению максимальной дальности действия NLJD целесообразно использовать имитатор ЗУ на базе двузаходовой плоской спиральной антенны (ПСА) [5], [6]. К центру антенны имитатора (точки А и В) подключен диод типа 2А604А (рис. 1). Выбор такого имитатора связан с его работоспособностью в широком диапазоне частот и эллиптической поляризацией плоских спиральных антенн. Спиральные антенны с коэффициентом перекрытия по частоте от 1,5 до 10 позволяют формировать однонаправленные ДН шириною 90°–180° с коэффициентом направленного действия (КНД) 2–8. Двузаходовая ПСА имитатора ЗУ спроектирована для диапазона частот 0,8–3 ГГц и изготовлена из фольгированого текстолита. Геометрические параметры ПСА имитатора: количество входов – 2; начальный радиус 22–26 мм; количество витков 2–3. В диапазоне частот 0,8–3 ГГц его диаграмма направленности изменяется (рис. 2, 3). На частоте 1 ГГц КНД соответствует 6,5–2,5 дБ при ширине главного лепестка ДН 90°–20°. На частоте 2 ГГц КНД соответствует 2,0–0,5 дБ при ширине главного лепестка ДН 120°–160°. На частотах выше 2 ГГц наблюдаются уменьшения КНД, вызванные расширением главного лепестка ДН.

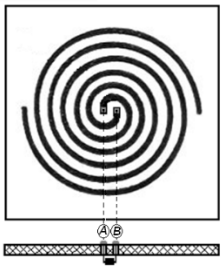


Рис. 1 – Имитатор

Действие СВЧ поля NLJD разной мощности P на указанный имитатор ЗУ может привезти к деформированию ВАХ диода. На рис. 4 представлена деформация ВАХ диода в составе имитатора ЗУ в случае использования NLJD типа “NR-μ” [7] (расстояние между имитатором и NLJD 0,5 м, действующая мощность ЗС 50−500 мВт, ВАХ диода измерялись комплексом МВУ8 [8]). Отметим, что в случае NLJD

типа “NR-μ” имеем круговую поляризацию ЗС, максимальная мощность сигнала зондирования в импульсе составляет 250 Вт на частоте 848 МГц, а чувствительность приёмника не превышает -140 дБ/Вт.

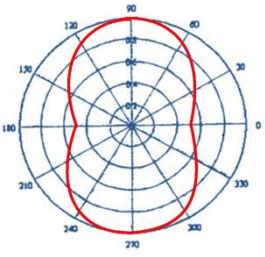


Рис. 2 – ДН на 1 ГГц

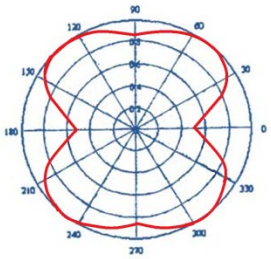


Рис. 3 – ДН на 2 ГГц

На рис. 4 деформация ВАХ имеет вид области с отрицательным дифференциальным сопротивлением (ОДС). Участок с ОДС характеризуется точками экстремума и шириной, отвечающей расстоянию между максимумом и минимумом.

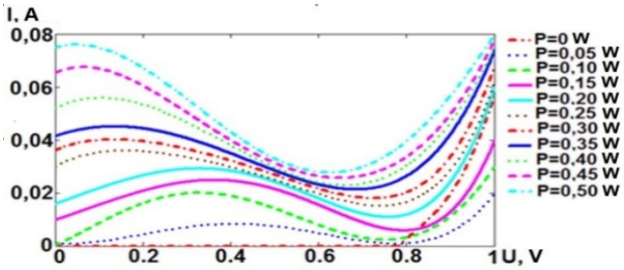


Рис. 4 – Деформирование ВАХ диода типа 2А604А при воздействии ЗС NLJD

Для этих трех параметров можно выделить общие закономерности в зависимости от уровня мощности действующего поля. С увеличением уровня действующей мощности точки экстремумов смещаются влево, а ширина ОДС увеличивается. Благодаря этому можно построить универсальное множество деформированных кривых в нормированных координатах в зависимости от приведенного значения коэффициента устойчивости γ_{ct}, $\gamma_{ct} \in [0;1]$,

$$\gamma_{ct} = (\gamma - \gamma_{\min}) / (\gamma_{\max} - \gamma_{\min}).$$

Такое универсальное множество кривых подлежит сопоставлению с деформированными ВАХ полупроводниковых элементов ЗУ при зондировании. Сопоставление аналитических и экспериментальных кривых предполагает масштабирование смоделированного множества и нахождение соответствий между значениями γ_{ct} и P.

Нормированную аппроксимирующую функцию (НАФ) деформированных ВАХ на рис. 4 представим в виде слагаемых функций: $F = F_1 + F_2 + F_3$. Функция F_1 описывает недеформированную форму ВАХ и начальную ее деформацию в зависимости от γ_{ct}. Функция F_2 для разных γ_{ct} описывает деформацию кривой параболической формы в диапазоне напряжений до точки минимума. Функция F_3 учитывает изменение крутизны области насыщения в зависимости от γ_{ct}. В итоге:

$$F_1(\gamma_{ct}, U_N) = \left(e^{11,3 \cdot U_N} - 1\right) \cdot \gamma_{ct}^5 \cdot 10^{-5};$$

$$F_2(\gamma_{ct}, U_N) = 0,35714 \times \\ \times e^{\sin\left(\left[A \cdot U_N + B \cdot (1 - 0,25 \cdot \gamma_{ct})\right]^3\right) - C \cdot \gamma_{ct}} \cdot (1 - \gamma_{ct});$$

$$F_3(\gamma_{ct}, U_N) = 0,082\left(e^{4,59 \cdot U_N \cdot (1 - \gamma_{ct})} - 1\right),$$

где A – параметр масштабирования формы кривой вдоль координаты U_N, B – параметр смещения кривой относительно U_N, C – параметр масштабирования семейства кривых по координате I_N.

Нахождение значений параметров масштабирования A, B и C выполняется в несколько этапов. На первом этапе нормированные экспериментальные данные представляются аналитически, например, в виде аппроксимирующих полиномов.

На втором этапе подбираются начальные значения параметров A, B и C для выбранных экспериментальных базисных кривых. Далее находятся базисные значения γ_{ct}, при которых наблюдаются

минимальные расхождения НАФ и аппроксимирующих полиномов.

На третьем этапе при фиксированных базисных значениях γ_{ct}. Значения каждого параметра A, B и C подлежит уточнению. Если НАФ базисных кривых имеют различия в параметрах масштабирования, то последние заменяются функциями (исходя из подобия промежуточных кривых). Для кривых на рис. 4 результаты поиска уточненных базисных НАФ приведены в табл. 1. Корректирующие функции, придающие подобие (инвариантность) промежуточным кривым:

$$A_0(\gamma_{ct}) = 0,265 \cdot \gamma_{ct}^2 + 3,062 \cdot \gamma_{ct} + 0,584;$$

$$B_0(\gamma_{ct}) = -4,229 \cdot \gamma_{ct}^2 - 1,217 \cdot \gamma_{ct} + 1,198.$$

Зависимость γ_{ct} от P представлена на рис. 5. Также на рисунке отображено изменение зависимости γ_{ct} от P при отклонении параметра C в большую сторону от уточненного значения. Полученные при исследовании имитатора ЗУ результаты обобщены на НРс с “малой” и “большой” НЭПР.

Таблица 1.

Уточненные параметры

P, мВт	A_0	B_0	C_0	γ_{ct}	ε
500	0,584	1,198	4	0,000	0,068
350	0,924	1,103	4	0,110	0,068
150	1,243	0,750	4	0,212	0,069

Примем, что НАФ и соотношение на рис. 5 для имитатора ЗУ соответствует нагрузкам разных антенных систем (приведенные значения γ_{ct} одинаковы при разных γ и $\gamma_{\min}$). Нормированная амплитуда наведенного напряжения ЗС U_{mN} (по максимальному напряжению ВАХ диода U_g) не превысит значение 0,1.

Применим к НАФ разложение Тейлора (использованы пять первых членов) и подставим функцию воздействия

$$U_N(t) = U_{0N} + U_{mN} \cdot \cos(\omega_0 t + \varphi),$$

где U_{0N} – нормированное напряжение смещения рабочей точки, ω_0 – круговая частота ЗС, φ – начальная фаза. В результате получим выражения нормированных уровней второй и третьей гармоник: $I_{2N} = f1(\gamma_{ct}, U_{mN}, U_{0N} = \text{const})$, $I_{3N} = f2(\gamma_{ct}, U_{mN}, U_{0N} = \text{const})$ (в силу громоздкости сами выражения не приводятся). В качестве примера, на рис. 6 приведены зависимости уровней второй и третьей гармоник сигнала отклика от γ_{ct}, U_{mN}, $U_{0N} = \text{const}$.

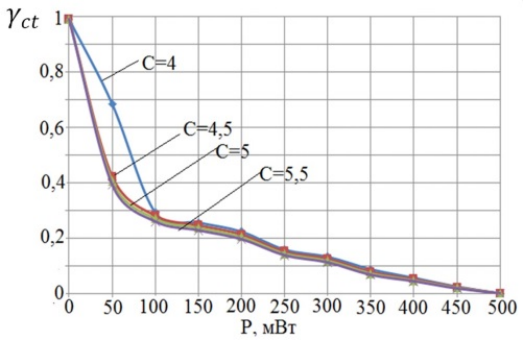


Рис. 5 – Соотношение коэффициента устойчивости и уровня мощности ЗС

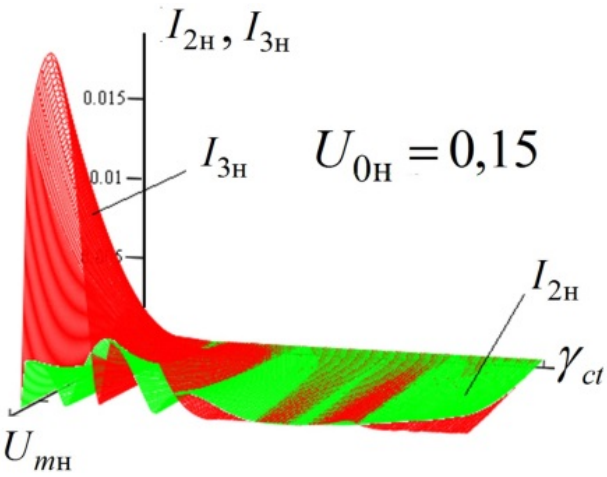
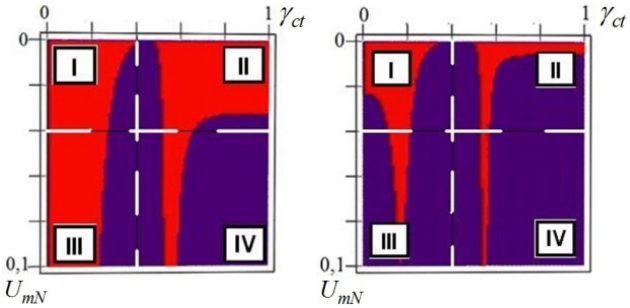


Рис. 6 – Распределения нормированных уровней кратных гармоник

Исследуем эффективность выявления и идентификации НРс относительно порогового соотношения L уровней второй и третьей гармоник СО. Для этого в координатах γ_{ct}, U_{mN} при $U_{0N} = 0,78$ (соответствует нелинейному участку недеформированной кривой НАФ)

построим поле $I_{2N}/I_{3N} > L$ (рис. 7). Как видно из рис. 7, для разных значений L характерны свои суммарные площади областей “надежной идентификации” в координатах γ_{ct}, U_{mN}.



$L = 26$ дБ $L = 40$ дБ

Рис. 7 – Распределение значений $I_{2N}/I_{3N} > L$ (светлые области)

Полученные поля значений $I_{2N}/I_{3N} > L$ разделены на четыре сектора (рис. 7). Первый сектор “I” ($\gamma_{ct} \in (0;0,4)$, $U_{mN} \in (0;0,04)$) соответствует НРс с “малой” НЭПР при зондировании “мощным” NLJD (присутствует деформация ВАХ диода). Второй сектор “II” ($\gamma_{ct} \in (0,4;1)$, $U_{mN} \in (0;0,04)$) отвечает НРс с “малой” НЭПР при зондировании “маломощным” NLJD (отсутствует деформация ВАХ диода). Третий сектор “III” ($\gamma_{ct} \in (0;0,4)$, $U_{mN} \in (0,04;0,1)$) отображает НРс с “большой” НЭПР при зондировании “мощным” NLJD. Четвертый сектор “IV” ($\gamma_{ct} \in (0,4;1)$, $U_{mN} \in (0,04;0,1)$) характеризует НРс с “большой” НЭПР при зондировании “маломощным” NLJD. Каждый сектор можно характеризовать усредненной шириной $\langle \gamma_{ct} \rangle_j$ области значений $I_{2N}/I_{3N} > L$ по координате γ_{ct} (светлые области на рис. 7), где j – порядковый индекс сектора (I, II, III и IV). Усредненным ширинам $\langle \gamma_{ct} \rangle_j$ соответствуют опорные значения U_{mN_j}, $\gamma_{ct_{1j}}$ и $\gamma_{ct_{2j}}$, по которым можно определить обобщенные свойства каждого сектора, где $\gamma_{ct_{1j}}$ и $\gamma_{ct_{2j}}$ – границы ширины области значений $I_{2N}/I_{3N} > L$ по координате γ_{ct} и опорному U_{mN_j}, $\Delta\gamma_{ct_j} = \gamma_{ct_{2j}} - \gamma_{ct_{1j}} = \langle \gamma_{ct} \rangle_j$. Согласно рис. 5 величины $\Delta\gamma_{ct_j}$, $\gamma_{ct_{1j}}$ и $\gamma_{ct_{2j}}$ можно перевести в соответствующие уровни мощности ЗС NLJD ($\Delta\gamma_{ct_j} \to \Delta P_j$, $\gamma_{ct_{1j}} \to P_{2j}$, $\gamma_{ct_{2j}} \to P_{1j}$, $\Delta P_j = P_{2j} - P_{1j}$).

Введем коэффициент эффективности порогового соотношения уровней второй и третьей гармоник сигнала отклика по каждому сектору

$$K_j = \frac{P_{2j} - P_{1j}}{P_{2j} + P_{1j}}.$$

Коэффициент K_j прямо пропорционален ширине $\Delta P_j = P_{2j} - P_{1j}$ и обратно пропорционален среднему уровню действующей мощности $\langle P_j \rangle = \left[P_{2j} + P_{1j} \right]/2$. Также K_j стремится к максимуму, если $P_{1j} \to 0$, поскольку для “маломощных” NLJD порог L служит критерием верной идентификации НРс. В табл. 2-5 для разных значений L по каждому сектору приведены опорные значения U_{mN_j}, P_{1j} и P_{2j}.

На рис. 8 приведено распределение значений коэффициента эффективности порогового соотношения уровней кратных гармоник K_j по секторам.

Таблица 2.

Параметры первого сектора

$T1$, дБ	$U_{mн_1}$	P_{2I}, мВт	P_{1I}, мВт
26	0,019	500	88
30	0,018	500	92
32	0,017	500	94
34	0,018	500	96
36	0,018	500	100
37	0.030	500	125
38	0,030	460	142
39	0,026	440	175
40	0,027	440	180

Таблица 3.

Параметры второго сектора

$T1$, дБ	$U_{тн_{II}}$	P_{2II}, мВт	P_{1II}, мВт
26	0,038	80	0
30	0,027	70	33
32	0,018	70	40
34	0,015	70	43
36	0,013	70	52
37	0,010	70	55
38	0,010	70	56
39	0,011	68	56
40	0,011	67	56

Таблица 4.

Параметры третьего сектора

$T1$, дБ	$U_{тн_{III}}$	P_{2III}, мВт	P_{1III}, мВт
26	0,070	500	150
30	0,078	490	180
32	0,068	370	170
34	0,066	330	200
36	0,070	310	210
37	0,082	290	210
38	0,083	280	212
39	0,071	275	220
40	0,069	270	225

Таблица 5.

Параметры четвертого сектора

$T1$, дБ	$U_{тн_{IV}}$	P_{2IV}, мВт	P_{1IV}, мВт
26	0,069	75	60
30	0,069	73	60
32	0,070	72	62
34	0,070	71	62
36	0,070	70	62
37	0,069	69	62
38	0,072	68	62
39	0,068	67	62
40	0,070	65	62

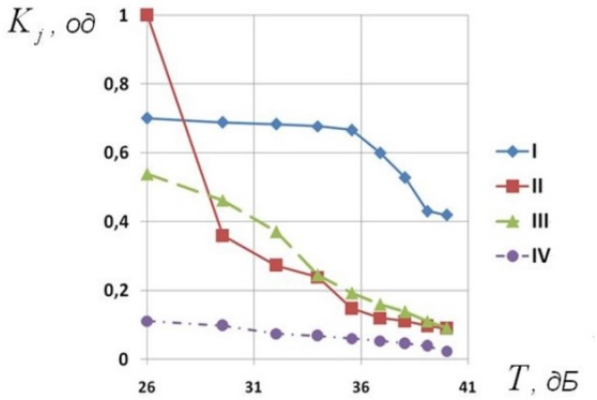


Рис. 8 – Распределение значений K_j по секторам

Из рисунка следует, что завышение порогового соотношения L (до 36 дБ) целесообразно лишь для “мощных” NLJD при зондировании НРс с “малой” НЭПР (первый сектор, $0{,}4 < K_1 < 0{,}7$ при $L = 20 - 40$ дБ). Порог L как критерий достоверной идентификации неэффективен для “маломощных” NLJD при зондировании НРс с “большой” НЭПР (четвертый сектор, $0{,}024 < K_1 < 0{,}111$ при $L = 20 - 40$ дБ). Для других случаев: “мощные” NLJD – рассеиватели с “большой” НЭПР (третий сектор) и “маломощные” NLJD – рассеиватели с “малой” НЭПР (второй сектор), пороговое соотношение L не должно превышать 28 дБ.

Выводы

Нелинейная радиолокация широко используются для выявления закладных устройств с радиоэлектронной элементной базой. Любое ЗУ является нелинейным рассеивателем. Детектор нелинейных переходов выявляет ЗУ по уровням кратных гармоник частоты зондирующего сигнала. Закладные устройства относительно длины волны ЗС NLJD делятся на НРс с “малой” и “большой” нелинейной эффективной площадью рассеивания. По излучаемому уровню мощности ЗС детекторы нелинейных переходов квалифицируются как “мощные” (импульсные) и “маломощные” (непрерывного действия). При достаточно высокой плотности

потока мощности ЗС вольт-амперная характеристика полупроводниковых элементов ЗУ испытывает деформацию. Деформация ВАХ имеет вид области с отрицательным дифференциальным сопротивлением. Введенный коэффициент устойчивости полупроводникового прибора на действие ЗС NLJD полностью характеризует область с ОДС. Характеристики участка с ОДС имеют зависимость от уровня мощности действующего поля. Экспериментально получены деформированные ВАХ диода имитатора ЗУ на базе двузаходовой плоской спиральной антенны. По результатам эксперимента найдено нормированную аппроксимирующую функцию множества деформированных ВАХ в зависимости от приведенного коэффициента устойчивости диода. Полученная НАФ подлежит обобщению на НРс с “малой” и “большой” НЭПР. При этом нагрузки разных антенных систем одинаково соотносятся между значениями приведенного коэффициента устойчивости и уровнями действующей мощности. С помощью обобщенной НАФ выведено выражение для нормированных уровней второй и третьей гармоник сигнала отклика. Это дает возможность исследовать эффективность достоверного обнаружения НРс по пороговому соотношению уровней кратных гармоник сигнала отклика. Результаты исследования показали, что завышение порогового соотношения (до 36 дБ) целесообразно лишь для “мощных” NLJD при зондировании НРс с “малой” НЭПР. Пороговое соотношение как критерий достоверной идентификации неэффективно для “маломощных” NLJD при зондировании НРс с “большой” НЭПР. В других случаях пороговое соотношение уровней кратных гармоник не должно превышать 28 дБ.

Перелік посилань

[1] В. А. Хорошко, А. А. Чекатков, *Методы и средства защиты информации*. К., 2003. 504 с.

[2] А. А. Горбачев, А. П. Колбанов, *Признаки распознавания нелинейных рассеивалелей электромагнитных волн,* Нелинейный мир 6. (2004). 301-309 с.

[3] М. В. Зінченко, Ю. Ф. Зіньковський, М. І. Прокофьєв, *Значущість рівня потужності зондуючого сигналу в нелінійній радіолокації,* Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні 1 (20) (2010). 102-113 с.

[4] K. M. Aliev, I. K. Kamilov, Kh. O. Ibragimova, *N-type negative differential resistance, hysteresis, and oscillations in the current-voltage characteristics of microwave diodes,* Semiconductors 46 (8) (2012). 1059-1065 s.

[5] М. В. Зінченко, Ю. Ф. Зіньковський *Широкосмугові розсіювачі в задачах нелінійної радіолокації,* Радіо-електроніка, інформатика, управління 1 (2016). 15-21 с.

[6] О. А. Юрцев, А. В. Рунов, *Спиральные антенны*. Москва, 1974. 224 с.

[7] *Измеритель спектра вторичных полей (детектор нелинейных переходов) «NR-μ»*. Руководство пользователя. 2010. 10 с.

[8] *МВУ8 ПО ОВЕН.* Руководство по эксплуатации. 2010. 70 с.

References

[1] V. A. Khoroshko, A. A. Chekatkov, *Metody y sredstva zashchyty ynformatsyy*. K., 2003. 504 s.

[2] A. A. Horbachev, A. P. Kolbanov, *Pryznaky raspoznavanyya nelyneynykh rasseyvaleley elektromahnytnykh voln,* Nelyneynyy myr 6. (2004). 301-309 s.

[3] M. V. Zinchenko, Yu. F. Zin'kovs'kyy, M. I. Prokof'yev, *Znachushchist' rivnya potuzhnosti zonduyuchoho syhnalu v neliniyniy radiolokatsiyi,* Pravove, normatyvne ta metrolohichne zabezpechennya systemy zakhystu informatsiyi v Ukrayini 1 (20) (2010). 102-113 s.

[4] K. M. Aliev, I. K. Kamilov, Kh. O. Ibragimova, *N-type negative differential resistance, hysteresis, and oscillations in the current-voltage characteristics of microwave diodes,* Semiconductors 46 (8) (2012). 1059-1065 s.

[5] M. V. Zinchenko, Yu. F. Zin'kovs'kyy *Shyrokosmuhovi rozsiyuvachi v zadachakh neliniynoyi radiolokatsiyi*, Radioelektronika, informatyka, upravlinnya 1 (2016). 15-21 s.
[6] O. A. Yurtsev, A. V. Runov, *Spyral'nye antenny*. Moskva, 1974. 224 s.
[7] *Yzmerytel' spektra vtorychnykh poley (detektor nelyneynykh perekhodov) «NR-μ».* Rukovodstvo pol'zovatelya. 2010. 10 s.
[8] *MVU8 PO OVEN.* Rukovodstvo po ekspluatatsyy. 2010. 70 s.

Реферат

Зінченко Максим; Во Зуй Фук;
Зіньковський Юрій; Прокофьєв Михайло

Співвідношення рівнів гармонік розсіяного поля у нелінійній радіолокації

У роботі розглянуті переваги використання методів нелінійної локації у сфері технічного захисту інформації. Показано, що пошук радіоелектронної апаратури як нелінійних розсіювачів (НРс) раціонально здійснювати детектором нелінійних переходів (NLJD – Non Linear Junction Detector). Ефективність використання NLJD пов'язана з вибором порогових значень співвідношень рівнів прийнятих кратних гармонік. Актуальною стає аналітична оцінка оптимальних значень порогів ідентифікації з врахуванням рівня діючої потужності зондуючого сигналу NLJD і нелінійної ефективної площі розсіювання (НЕПР) закладного пристрою. Для цього доцільно використовувати імітатор закладного пристрою на базі двозаходової плоскої спіральної антени з напівпровідниковим діодом у навантаженні. Діюче на імітатор НВЧ поле від NLJD призводить до деформації вольт-амперної характеристики діода. В процесі досліджень виявлено, що завищення порогового значення демаскуючої ознаки доцільне лише для "потужних" випромінювань NLJD при зондуванні НРс з "малою" НЕПР. Поріг як критерій достовірної ідентифікації неефективний для "малопотужних" випромінювань NLJD при зондуванні НРс з "великою" НЕПР.

Зинченко Максим; Во Зуй Фук;
Зиньковский Юрий; Прокофьев Михаил

Соотношения уровней гармоник рассеяного поля в нелинейной локации

В работе рассмотрены преимущества применения методов нелинейной локации в сфере технической защиты информации. Показано, что поиск радиоэлектронной аппаратуры как нелинейных рассеивателей (НРс) рационально осуществлять детектором нелинейных переходов (NLJD – Non Linear Junction Detector). Эффективность использования NLJD связана с выбором пороговых значений соотношений уровней принятых кратных гармоник. Актуальной становится аналитическая оценка оптимальных значений порогов идентификации с учетом уровня действующей мощности зондирующего сигнала NLJD и нелинейной эффективной площади рассеивания (НЭПР) закладного устройства. Для этого целесообразно использовать имитатор закладного устройства на базе двузаходовой плоской спиральной антенны с полупроводниковым диодом в нагрузке. Воздействующее на имитатор СВЧ поле от NLJD приводит к деформированию вольт-амперной характеристики диода. В процессе исследований выявлено, что завышение порогового значения демаскирующего признака целесообразно лишь для "мощных" излучений NLJD при зондировании НРс с "малой" НЭПР. Порог как критерий достоверной идентификации неэффективен для "маломощных" излучений NLJD при зондировании НРс с "большой" НЭПР.

Zinchenko Maksym; Vo Duy Phuc;
Zinkovskiy Yuriy; Prokofiev Mikhail

The ratio of harmonics levels of the scattered field in nonlinear locations

The article discusses about the advantages of using the methods of nonlinear location in the field of technical protection of information. It is shown that searching for radio electronic equipment as a nonlinear scattered (NS) efficiently implement the Non Linear Junction Detector (NLJD). The efficiency of NLJD associated with the choice of thresholds of the ratio of the received multiple harmonics levels. It becomes relevant analytical estimation of the optimal values of the thresholds of identification, with considering the power level of the probing signal of NLJD and the non-linear effective square of scatterer of mortgaged devices. It is advisable to use the simulator of mortgaged device on the basis of two-way flat spiral antenna with semiconductor diode in the load. Working on the simulator in the microwave field from NLJD leads to deformation of the current-voltage characteristics of the diode. During the investigations, it was found that the overestimation of threshold is only suitable to mask for "high-power" NLJD radiation in probing the LDCs with a "small" non-linear effective square of scatterer. The threshold is a criterion of reliable identification of inefficient for "low-power" NLJD radiation in probing the NS with the "big" non-linear effective square of scatterer.

Відомості про авторів

Зіньковський Юрій Францевич
Освіта: Вища повна (1956).
Науковий ступінь: Доктор технічних наук.
Вчене звання: Професор.
Місце роботи: Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського».
Область знань: Технічні науки.
Наукові інтереси: Радіоелектроніка, мікроелектроніка; технічний захист інформації; комп'ютерне проектування радіоелектронної апаратури, технологія електронного апаратобудування; педагогіка вищої освіти.
Email: *krasan@ukr.net*

Зінченко Максим В'ячеславович
Освіта: Вища повна (2009).
Науковий ступінь: Кандидат технічних наук.
Місце роботи: Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського».
Область знань: Технічні науки.
Наукові інтереси: Радіоелектроніка, мікроелектроніка; технічний захист інформації; комп'ютерне проектування радіоелектронної апаратури, технологія електронного апаратобудування; педагогіка вищої освіти.
Email: *zil157k@meta.ua*

Во Зуй Фук
Освіта: Вища повна (2012).
Місце роботи: Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського».
Область знань: Технічні науки.
Наукові інтереси: Радіоелектроніка, мікроелектроніка; технічний захист інформації; комп'ютерне проектування радіоелектронної апаратури, технологія електронного апаратобудування; педагогіка вищої освіти.
Email: *voduyphuc@bigmir.net*

Прокофьєв Михайло Іванович
Освіта: Вища повна (1972).
Науковий ступінь: Кандидат технічних наук.
Місце роботи: Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», директор Науково-дослідного центру «ТЕЗІС».
Область знань: Системи захисту інформації.
Наукові інтереси: Інформаційна безпека, системи захисту інформації, проектування радіоелектронної апаратури та систем.
Email: *pmi@tesis.kiev.ua*

УДК 621.396.4

НАТУРНІ ВИПРОБУВАННЯ СТАНЦІЇ ТРОПОСФЕРНОГО ЗВ'ЯЗКУ

Гнатюк Сергій; Вергелес Дмитро; Гуменюк Володимир; Паламарчук Андрій; Стефанишин Ярослав
Державний науково-дослідний інститут спеціального зв'язку та захисту інформації

THE NATURE TESTING OF TROPOSCATTER COMMUNICATION STATION

Gnatiuk Sergii; Vergeles Dmytro; Gumenyuk Volodymyr; Palamarchuk Andriy; Stefanyshyn Yaroslav
State Research Institute for Special Telecommunication and Information Protection

Аннотація: **Наведено результати натурних випробувань станції тропосферного зв'язку у радіолокаційному режимі, які експериментально підтверджені у реальних умовах.**
Ключові слова: **Тропосферний зв'язок, дальність радіозв'язку, натурні випробування, радіолокаційний режим, передавач та приймач станції тропосферного зв'язку.**
Summery: **Presented the results of nature testing of troposcatter communication station on the radar mode.**
Keywords: **Troposcatter communication, radio coverage, nature testing, radar mode, transmitter and receiver of troposcatter communication station.**

Вступ

Станції тропосферного зв'язку забезпечують передавання дискретної інформації зі швидкістю до 10 Мбіт/с на відстань понад 2000 км з інтервалами між станціями 70 – 300 км. Свого часу вони слугували одним із надійних засобів зв'язку, але за останні 10–20 років, зважаючи на бурхливий розвиток космічних телекомунікаційних засобів, тропосферні станції майже втратили комерційну привабливість. На поточний час вони вважаються перспективними для оперативного створення радіоліній у надзвичайних умовах, а також спеціальних ліній зв'язку, які забезпечують діяльність силових структур. Крім того, тропосферні станції мають певні перспективи при забезпеченні зв'язком у важкодоступних та малонаселених районах, які знаходяться у високоширотних областях земної поверхні.

Сучасна елементна база надає можливості для значного спрощення технічної реалізації тропосферних станцій, проте вони залишаються складними пристроями, які потребують виконання достатньо великих обсягів випробувань для забезпечення умов надійного радіозв'язку (у тому числі і натурних). Технічна складність тропосферних станцій обумовлена характером поширення хвиль у радіолінії (нестабільність тропосфери, багатопроменевість, велика ймовірність спотворення інформаційних потоків, значні енергетичні втрати), а також проблемами вимірювання значень параметрів створюваної радіолінії [1], [2].

Особливістю вимірювання значень параметрів тропосферної станції є технічна складність практичного створення імітаторів тропосферного поширення радіохвиль. Тому на практиці для проведення випробувань у регіонах, в яких передбачається експлуатація станції, необхідно створювати довгострокові випробувальні полігони [3], [4]. Для випробувань станцій прямої видимості вже розроблено ряд методик, обладнання та імітаторів, які дозволяють проводити випробування на обмежених площах (закриті полігони, стендові зали, виробничі приміщення тощо). Але натурні випробування тропосферних станцій

потребують додаткових трудових та фінансових витрат і тому реалізація цієї задачі проблематична.

Перш за все, при натурних випробуваннях тропосферних станцій необхідно забезпечити реальні відстані між їх приймальною та передавальною частинами (100 – 200 км). А саме це пов'язано з певними незручностями, що обумовлюються неможливістю одночасного доступу персоналу до її приймальної і передавальної частин для проведення регулювальних та вимірювальних робіт (що важливо на початкових етапах створення будь-якого технічного засобу зв'язку, у тому числі і тропосферної станції).

Метою проведених авторами досліджень було визначення можливості натурних випробувань тропосферної станції у радіолокаційному режимі – при розміщенні її приймальної та передавальної частин на невеликій відстані (практично, в одному місці).

Основна частина

Обгрунтування методу натурних досліджень тропосферної станції. В основі методу натурних досліджень тропосферної станції у радіолокаційному режимі лежать роботи, які проводилися впродовж тривалого проміжку часу багатьма авторами [2].

Загалом, можливість тропосферного радіозв'язку пов'язана з явищем розсіювання електромагнітних хвиль на локальних неоднорідностях атмосфери, які характеризуються різною діелектричною проникливістю, що виникає внаслідок турбулентності атмосфери і залежить від її вологи, температури та тиску.

При падінні хвилі радіовипромінювання на локальні неоднорідності діелектричної проникливості у тропосфері виникає електромагнітне поле різноспрямованого розсіювання. Якщо неоднорідність діелектричної проникливості представити як антену, яка рівномірно опромінюється полем пласкої хвилі, то при розмірах неоднорідності, що значно перевищує довжину хвилі, інтенсивність вторинного поля розсіювання такої «антени» характеризується нерівномірним розподілом у просторі. Зокрема, основне розсіювання первинної хвилі спрямоване у напрямі руху радіохвилі і затухає у просторі, а деяка його частина розсіюється у бокових (у тому числі і у зворотньому) напрямах. Крім того, у реальній атмосфері на шляху поширення радіохвилі зустрічаються хаотичні рухомі неоднорідності діелектричної проникливості різних розмірів і інтенсивностей. Підсумкове поле розсіювання радіохвиль на цих неоднорідностях характеризується діаграмою розсіювання, в якій радіохвилі поширюються в у всіх напрямах. При цьому розсіяна енергія радіохвиль досягає тих ділянок на земній поверхні, з яких ці неоднорідності діелектричної проникливості будуть «видимими». Схематично розсіювання радіохвиль на діелектричних неоднорідностях тропосфери наведено на рис. 1.

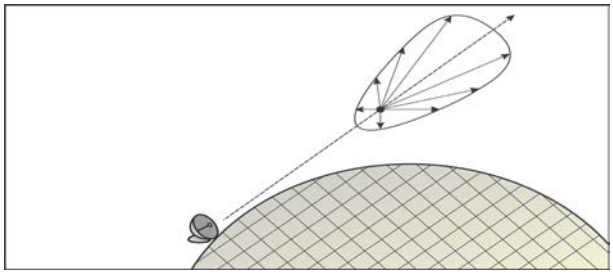


Рис. 1 – Схема розсіювання радіохвиль на діелектричних неоднорідностях тропосфери

Таким чином, у процесі розсіювання радіохвиль тропосферою бере участь певна поверхня нестабільного об'єму (ефективна поверхня розсіювання – ЕПР), яка знаходиться у просторі, обмеженому перетином променів діаграм спрямованості передавальної та приймальної антен.

Підсумкове поле у місці приймання розсіяного тропосферою сигналу визначається сумою значень енергій (з урахуванням амплітуди та фази) парціальних радіохвиль, що розсіюються окремими неоднорідностями «видимими» з передавального та приймального пунктів, наслідком чого є явища багатопроменевості та федингу (затухання) прийнятого сигналу

у точці приймання.

Приймання сигналу, розсіяного у зворотньому напрямі, дає можливість випробувати тропосферну станцію з розташуванням її приймальної та передавальної частин практично у одному місці.

Вибір місця проведення випробувань. Для проведення натурних випробувань доцільно використовувати невелику відкриту ділянку, розміщену на підвищені, що господарює над місцевістю та (для зменшення кута закриття горизонту) віддалена від місцевих предметів значних розмірів на відстань не менше 1,5 км. Бажано врахувати також те, що завади (лісові насадження, щільна міська забудова, а також окремі будівлі) у метровому діапазоні електромагнітного спектру частот необхідно розглядати як непрозорі, незважаючи на те, що в більш низькочастотних діапазонах лісові масиви можуть розглядатися як напівпрозорі.

Реально випробувальна ділянка розміщувалась на даху 9-поверхового будинку з випромінюванням у бік лісового масиву, у напрямі якого були відсутні завади.

Розміщення технічних засобів при випробуваннях. Для випробувань використовувалися макети передавальної та приймальної частин тропосферної станції, функціональні схеми яких наведені на рис. 2 та рис. 3 відповідно.

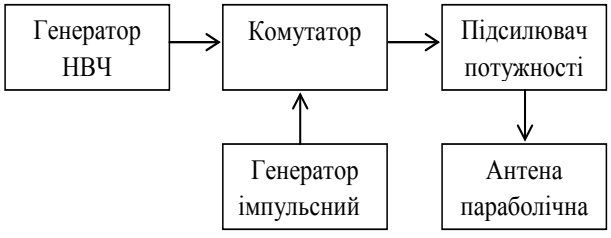


Рис. 2 – Схема макету передавальної частини тропосферної станції

При проведенні випробувань за допомогою генератора НВЧ забезпечувалася генерація сигналу з частотою 4,5 ГГц та потужністю близько 0 дБмВт, який модулювався імпульсним комутатором (протяжність імпульсу – 21 мкс, період повторення – 1000 мкс) і після підсилення підсилювачем потужності (коефіцієнт підсилення близько 50 дБ, вихідна потужність – близько 80 Вт) випромінювався через параболічну антену (коефіцієнт підсилення близько 34 дБ). Комутатор було виконано на базі мікросхеми HMC270AMS9G Hittite Microwave products, а керування ним забезпечувалося імпульсним генератором НМ 8130. Протяжність імпульсу визначалась протяжністю кодової комбінації, яку передбачається обробляти узгодженими фільтрами на поверхневих акустичних хвилях у створюваній станції тропосферного зв'язку. Частота повторення визначалась максимальною дальністю радіозв'язку (при подвійному проходженні сигналом траси – близько 300 км).

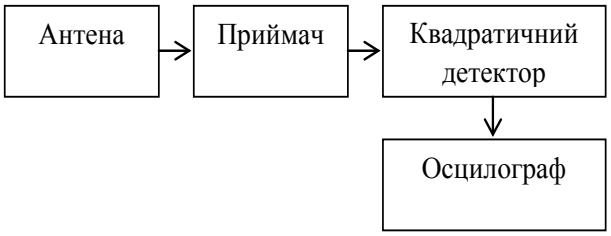


Рис. 3 – Схема макету приймальної частини тропосферної станції

Сигнал, прийнятий приймачем (чутливість не гірше «мінус» 110 дБВт) з параболічною антеною (коефіцієнт підсилення не менше 34 дБ) детектувався квадратичним детектором (виконано на базі перемножувала AD8341R) і фіксувався осцилографом (Tektronix TDS1012).

Схему орієнтації і розміщення передавальної та приймальної частин макетного зразка тропосферної станції при випробуваннях наведено на рис. 4.

Для забезпечення перетину пелюстків діаграм спрямованості передавальної та приймальної антен одна з них (передавальна) встановлювалась за азимутом 10^0 та кутом місця $5{,}5^0$, а для приймальної забезпечувалася можливість регулювання за азимутом близько $(5.5\pm0{,}5)^0$ та кутом місця $(10\pm1)^0$ на відстані близько 50 м (що обумовлено рівнем бокових пелюстків їх діаграм спрямованості та побічними випромінюваннями). Відстані визначені експериментально.

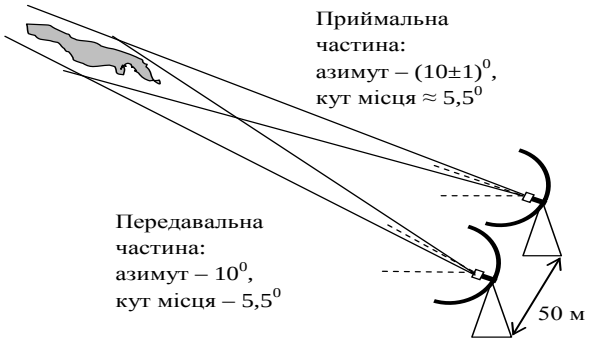


Рис. 4 – Схема орієнтації і розміщення передавальної та приймальної частин макетного зразка тропосферної станції

Проведення випробувань. Одним із основних завдань, яке вирішувалось при випробуваннях, було підтвердження прийнятих технічних рішень щодо рівня ефективної ізотропної випромінюваної потужності (ЕІВП) для забезпечення заданого інтервалу зв'язку при тропосферному поширенні сигналу. При цьому, інтервал зв'язку визначався затримкою між переднім фронтом випромінюваного імпульсу та передніми фронтами прийнятих імпульсів. Отримання необхідних затримок досягалося шляхом регулювання азимуту та кута місця приймальної антени, що давало можливість фактично змінювати відстань до місця перетину пелюстків діаграми спрямованості антен.

Осцилограма сигналів на виході приймача при кутах місця передавальної та приймальної антен близько 5,5^0 та азимуті – близько 10^0 (точне вимірювання кутів не забезпечувалося) наведена на рис. 5. На осцилограмі можна візуально виділити 4 відбиті сигнали (показано стрілкою), які прийшли на вхід приймача різними шляхами (променями), відбитими тропосферою з затримкою 620 мкс та більше (відстань – орієнтовно, 180 км).

Загалом, випробування проводилися у режимі випромінювання частоти-носія. Разом з тим, після досягнення необхідних орієнтацій антен є реальна можливість забезпечити випробування тропосферної станції при передаванні інформації з визначенням параметрів створеної радіолінії (наприклад, мінімальне відношення сигнал/шум при якому забезпечується заданий коефіцієнт бітової помилки).

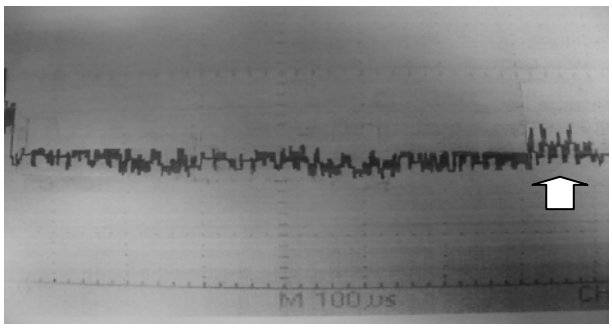


Рис. 5 – Осцилограма сигналів на виході приймальної частини тропосферної станції

Отримані результати були підтверджені при рознесенні передавальної та приймальної частин станції на визначені відстані (150-180 км). Це свідчить про можливість проведення попередніх випробувань створюваних станцій тропосферного зв'язку у радіолокаційному режимі.

Висновки

Додаткове включення до складу станції тропосферного зв'язку амплітудного модулятора та генератора імпульсних сигналів (який забезпечує управління цим модулятором) дає можливість реалізувати радіолокаційний режим роботи станції та провести її натурні випробування при розміщенні передавальної та приймальної частин, практично, у одному місці (що доцільно на початкових етапах її створення).

Перелік посилань

[1] В. В. Серов, *Особенности распространения радиоволн в загоризонтных системах радиосвязи.* – Электросвязь, 2009, №1.

[2] *Дальнее тропосферное распространение ультракоротких радиоволн.* Под ред. Б. А. Введенского. – М., Советское радио, 1965.

[3] *Справочник по радиорелейной связи.* Под ред. С. В. Бородича. – М., Радио и связь, 1981.

[4] *Справочник по спутниковой связи.* Под ред. С. В. Бородича. – М., Радио и связь, 1986.

[5] Ю. И. Давыденко, *Дальняя тропосферная связь.* — М: Воениздат, 1968.

References

[1] V. V. Serov, *Osobennosti rasprostranenia radivoln v zagorizontnyh sistemah radiosviazi.* – Elektrosviaz, 2009, #1.

[2] *Dalnee troposfernoe rasprostranenie ultrakorotkih voln.* Pod red. B. A. Vvedenskogo. – M. Sovetskoe radio,1955.

[3] *Spravochnik po radioreleynoy sviazi.* Pod red. S. V. Borodicha. –. M. Radio i sviaz, 1981.

[4] *Spravochnik po sputnikovoy sviazi.* Pod red. S. V. Borodicha. –. M. Radio i sviaz, 1986.

[5] Yu. I. Davidenko, *Dalnyaia troposfernaia sviaz*, – M., Voenizdat, 1968.

Реферат

Гнатюк Сергій; Вергелес Дмитро; Гуменюк Володимир; Паламарчук Андрій; Стефанишин Ярослав

Натурні випробування станції тропосферного зв'язку

В статті стисло обґрунтовано можливість та наведено результати натурних випробувань станції тропосферного зв'язку у радіолокаційному режимі, які експериментально підтверджені у реальних умовах. Введення до складу передавача імпульсного модулятора (протяжність імпульсу – 21 мкс, період повторення – 1000 мкс) дало можливість на виході приймача, розташованого на відстані 50 м, отримати низку сигналів, відбитих від тропосфери, з еквівалентним інтервалом розповсюдження близько 180 км. Зроблено висновок щодо доцільності проведення таких випробувань на початкових етапах створення станції тропосферного зв'язку.

Гнатюк Сергей; Вергелес Дмитрий; Гуменюк Владимир; Паламарчук Андрей; Стефанищин Ярослав

Натурные испытания станции тропосферной связи

В статье кратко обоснована возможность и приведено результаты натурных испытаний станции тропосферной связи в радиолокационном режиме. Включение в состав передатчика импульсного модулятора (длительность импульса – 21 мкс, период повторения – 1000 мкс) дало возможность на выходе приемника, расположенного на расстоянии 50 м, получить пачку сигналов, отраженных от тропосферы, с эквивалентным интервалом распространения около 180 км. Сделано заключение о целесообразности проведения таких испытаний на начальных этапах создания станции тропосферной связи.

Gnatiuk Sergii; Vergeles Dmytro; Gumenyuk Volodymyr; Palamarchuk Andriy; Stefanyshyn Yaroslav

The nature testing of troposcatter communication station

Presented the results of nature testing of troposcatter communication station on the radar mode. Annexation to transmitter the impulse modulator (pulse duration – 21 μs, oscillation period – 1000 μs) to do possible on the receiver output, in line 50 m, to take the troposphere signals with equivalent distance 180 km. Make a conclusion about expediency to realization these tests on the initial design stages of troposcatter communication station.

Відомості про авторів

Гнатюк Сергій Євгенович
Освіта: Повна вища, Радіофізика і електроніка (1996).
Науковий ступінь: Кандидат технічних наук (2016).
Місце роботи: Державний науково-дослідний інститут спеціального зв'язку та захисту інформації.
Область знань: Радіофізика і електроніка.
Наукові інтереси: Системи захисту інформації.

Вергелес Дмитро Дмитрович
Освіта: Повна вища**,** Радіорелейні та тропосферні засоби зв'язку (1981).
Місце роботи: Державний науково-дослідний інститут спеціального зв'язку та захисту інформації.
Область знань: Засоби радіотехнічного зв'язку та передачі інформації.
Наукові інтереси: Системи зв'язку та радіолокації.

Гуменюк Володимир Іванович
Освіта: Повна вища, Машинобудування (1994).
Місце роботи: Державний науково-дослідний інститут спеціального зв'язку та захисту інформації.
Область знань: Конструювання та розроблення засобів технічного захисту інформації.
Наукові інтереси: Розроблення зразків військової та спеціальної техніки.

Паламарчук Андрій Андрійович
Освіта: Електроакустика і ультразвукова техніка (1967).
Науковий ступінь: Кандидат технічних наук (1987).
Місце роботи: Державний науково-дослідний інститут спеціального зв'язку та захисту інформації.
Область знань: Засоби радіотехнічного зв'язку та передачі інформації.
Наукові інтереси: Системи зв'язку та радіолокації.

Стефанишин Ярослав Іванович
Освіта: Конструювання радіоапаратури (1973).
Місце роботи: Державний науково-дослідний інститут спеціального зв'язку та захисту інформації.
Область знань: Засоби радіотехнічного зв'язку та передачі інформації.
Наукові інтереси: Системи зв'язку та радіолокації.
Email: *yaroslavstf@ukr.net*

УДК 004.056.53:621.3

ОСОБЛИВОСТІ ВИМІРЮВАННЯ ПАЧОК ПЕРІОДИЧНИХ ІМПУЛЬСНИХ СИГНАЛІВ ЗА ДОПОМОГОЮ АНАЛІЗАТОРА СПЕКТРУ

Стеченко Василь; Танцюра Денис
НДЦ "ТЕЗІС" КПІ ім. Ігоря Сікорського

FEATURES OF MEASURING THE LAYER OF PERIODIC PULSE SIGNALS BY THE SPECTRA ANALYZER

Stechenko Vasil; Tantsyura Denis
SRC «TESIS» Igor Sikorsky Kyiv Polytechnic Institute

Анотація: **Розглянуто особливості вимірювання аналізатором спектру гармонік пачок імпульсів малого рівня. Показано шлях визначення поправки на яку треба збільшувати результати вимірювань для визначення рівня гармоніки в пачці імпульсів.**
Ключові слова: **побічні випромінювання, поправка для розрахунку гармонік імпульсів.**
Summary: **The peculiarities of measuring the harmonics of small-scale pulses of pockets are considered. A way of determining the correction for which it is necessary to increase the measurement results to determine the harmonic level in a packet of pulses is shown.**
Keywords: **Emission, correction for calculation of harmonics of impulses.**

Вступ

Визначення рівня малих, в порівнянні з рівнем шуму, імпульсних сигналів здійснюється шляхом передавання тестової послідовності як періодичної послідовності імпульсів і пауз з подальшим вимірюваням рівня гармонік такої послідовності за допомогою аналізатора спектру. За рахунок зменшення смуги пропускання фільтра проміжних частот (ПЧ) підвищується чутливість аналізатора спектру, що дозволяє виявити гармоніки періодичної послідовності імпульсів малого рівня.

Під час вимірювання рівнів побічного випромінювання засобів електронно-обчислювальної техніки (ЕОТ) періодична послідовність імпульсів з паузами створюється шляхом передавання спеціальних тестових файлів, даних які кодуються шляхом періодичного повторення імпульсів мінімальної тривалості. Довжина пачок і час їх повторення обмежені стандартом прийнятого інтерфейсу передавання даних в ЕОТ.

Типові аналізатори спектру призначені для вимірювання та аналізу рівнів гармонік періодичних сигналів, значення параметрів яких залишаються незмінними за час вимірювання. Для пачок імпульсів з паузами результати вимірювань стають залежними від значень параметрів налаштувань аналізатора: швидкості сканування, смуги пропускання, типу детектора, тощо. Визначенню поправки для перерахунку при вимірювання рівня гармоніки у пачці імпульсів і присвячена ця стаття.

Структурна схема аналізатора спектру

Спрощено аналізатор спектру можна представити у вигляді фільтру, центральна частота якого періодично сканує в смузі огляду. Сканування здійснюється шляхом перестроювання частоти гетеродину (рис. 1), за допомогою якого сигнал переноситься на постійну проміжну частоту. В підсилювачі ПЧ сигнал підсилюється, фільтрується, детектується, а його рівень відображається на індикаторі.

Внаслідок сканування вимірювання рівня конкретної гармоніки сигналу здійснюється не постійно, а з паузами. В сучасних аналізаторах ще додається пауза для цифрової обробки виміряних значень сигналу. Довжина цих пауз в аналізаторах з цифровою обробкою сигналу значно перевищує час вимірювання. Періодичний режим вимірювання з паузами не впливає на точність вимірювань рівнів гармонік безперервних сигналів, але це не стосується пачок імпульсних послідовностей.

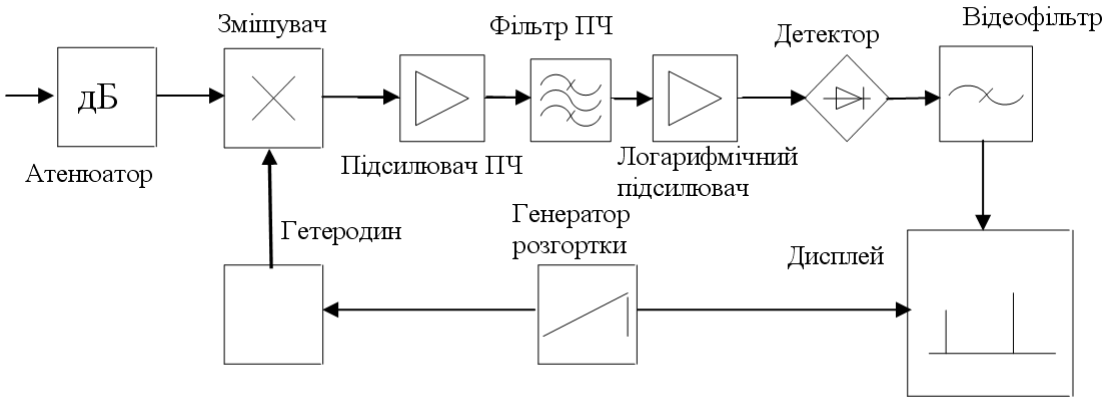


Рис. 1 – Структурна схема аналізатора спектру гетеродинного типу

Основними параметрами аналізатора спектру є: час розгортки $T_р$, смуга огляду ΔF і смуга пропускання фільтру ПЧ $B_{пч}$, тип фільтру ПЧ (Гауса, Батерворта, тощо), тип детектора (миттєвих, максимальних, середніх значень, квадратичний детектор, тощо). Час розгортки $T_р$, смуга огляду ΔF і смуга пропускання $B_{пч}$ пов'язані між собою співвідношенням [1]:

$$T_р = k \cdot \frac{\Delta F}{B_{пч}^2} \cdot k_{обр} = \frac{k}{B_{пч}} \cdot \frac{\Delta F}{B_{пч}} \cdot k_{обр} = t_{вим} \cdot n \cdot k_{обр} \quad (1)$$

де k – коефіцієнт пропорційності, значення якого залежить від типу фільтру та допустимої похибки визначення рівня сигналу. Типове значення $k_1 = 2{,}5$; $t_{вим}$ – час вимірювань однієї частотної точки; n – кількість точок вимірювань за один період сканування; $k_{обр}$ – збільшення часу на цифрову обробку виміряних даних та їх індикацію. Час розгортки, зазвичай, встановлюється автоматично після вибору смуги огляду ΔF і смуги пропускання $B_{пч}$.

Вимірювання пачок періодичних імпульсів

Сканування центральної частоти аналізатора спектру та існування пауз між пачками імпульсів призводить до випадковості часу початку сканування і часу появи пачки тестового сигналу. Для окремого періоду сканування на час вимірювань рівня гармоніки сигналу можлива поява усієї пачки імпульсів (залежність 1 на рис. 1), частини пачки (залежність 3) або повна її відсутність (залежність 2).

Відповідно рівень сигналу на виході детектора у кожному випадку буде різним, хоча рівень гармоніки у пачці імпульсів залишалася незмінною. За рахунок різниці частоти сканування і частоти повторення пачок імпульсів момент початку вимірювань наблизиться до моменту появи пачки, але неможливо одразу визначити необхідну кількість циклів сканування.

Для повного наростання сигналу в резонансному фільтрі ПЧ смуга його пропускання повинна перевищувати значення $B_{пч} = (2{,}5\text{-}3)/t_п$, де $t_п$ – тривалість пачки імпульсів. При менших значеннях смуги $B_{пч}$ амплітуда коливань на виході фільтра ПЧ не встигає досягти свого максимального значення і для визначення дійсного рівня сигналу потрібна корекція результатів вимірювань. Для імпульсних відеосигналів пропонується для корекції поправочний коефіцієнт визначати за формулою [1]:

$$\Delta K = 20\lg(k_ф t_п B_{пч}), \qquad (2)$$

де $k_ф = 1{,}5$ для прямокутного фільтру ПЧ та $k_ф = 1$ для Гаусового фільтру. Для радіоімпульсів значення коефіцієнту $k_ф$ треба збільшувати у 2 рази.

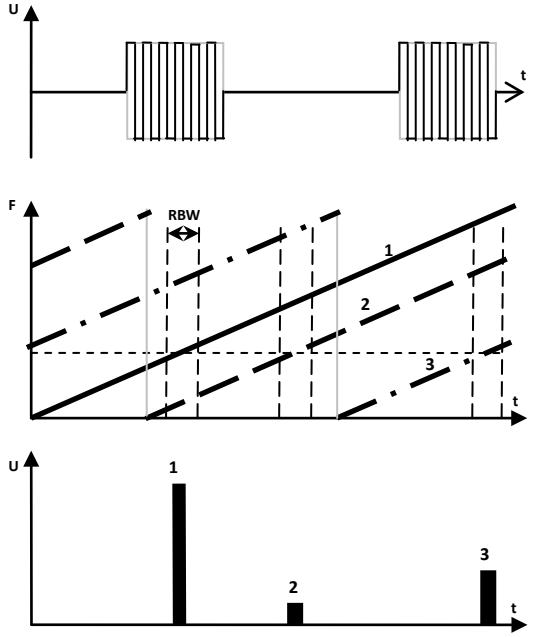


Рис. 2 – Залежність результатів вимірювання імпульсних сигналів від часу запису:
1 – співпадіння часу вимірювання відповідного рівня гармоніки у пачці сигналів з моментом появи пачки;
2 – відсутність пачки сигналів на час вимірювання рівня гармоніки (результат вимірювань – рівень шуму);
3 – часткове співпадіння часу вимірювання з моментом появи пачки

Для імпульсних сигналів тип детектора впливає на результати вимірювань рівня гармонік. Для детектора миттєвих значень виміряний рівень гармоніки буде змінюватися в залежності від різниці у часі між часом вимірювань і часом появи пачки. Детектор середніх значень буде зменшувати межі коливань результатів вимірювань. Детектор з фіксацією максимальних значень (MAX HOLD) буде накопичувати і запам'ятовувати найбільші значення багаторазових вимірювань. Тому кінцевий результат буде відповідати найбільш близькому співпадінню моменту появи пачки з моментом вимірювання спектру на частоті гармоніки. Необхідну кількість циклів сканування легко визначити шляхом контролю за моментом зупинення наростання виміряного рівня гармоніки.

Часто тривалість пачки t_n імпульсів невідома. В такому разі необхідну смугу пропускання $B_{пч}$ теж слід визначити експериментально. Якщо збільшення смуги $B_{пч}$ не проводить до зростання виміряного значення рівня гармоніки в режимі фіксації максимальних значень, то це означає, що виконується критерій $B_{пч} > 3/t_n$ і за час вимірювання рівень гармоніки встигає досягти свого максимального значення. При цьому результат вимірювань рівня гармоніки у пачці співпадає з рівнем гармоніки нескінченної послідовності імпульсів.

Нажаль вимірювання рівня гармоніки з широкою смугою пропускання та в режимі фіксації значень максимального рівня можливо тільки для імпульсних сигналів достатньо високого рівня, оскільки рівень шумової доріжки збільшується пропорційно $\sqrt{B_{пч}}$. При цьому ще фіксується суміш сигналу з максимальним значенням шуму, який приблизно на 10 дБ вище за його середньоквадратичне значення.

Для підвищення чутливості аналізатора спектру слід зменшувати смугу пропускання фільтру ПЧ і використовувати режим усереднення результатів багаторазових вимірювань. При цьому пропорційно $\sqrt{B_{пч}}$ падає рівень шумової доріжки, підвищується чутливість аналізатора спектру і відкривається можливість виявлення гармонік сигналу малого рівня. Типово під час вимірювань використовується логарифмічна шкала відліку. Тоді за рахунок усереднення логарифмічних даних, рівень виміряного шуму стає ще на 2,5 дБ меншим за його середньоквадратичне значення [1]. Таким чином, при однакових смугах пропускання перехід до режиму усереднення зменшує рівень шумової доріжки більш ніж на 12 дБ в порівнянні з вимірюванням з фіксацією максимальних значень. Але одночасно зі зменшенням рівня шумової доріжки

зменшується і виміряний рівень гармоніки, оскільки за час існування пачки амплітуда коливань сигналу в резонансному фільтрі ПЧ не встигає досягнути свого максимального значення.

Крім того зі зменшенням смуги $B_{пч}$ збільшується час вимірювання. Цей час може зрости настільки, що він буде охоплювати декілька періодів повторювання пачок імпульсів. При цьому відсутні пропуски пачок імпульсів і тому зменшується вплив на результати вимірювання фази між початком сканування і часом появи пачки тестового сигналу. Є межа, при досягненні якої подальше зменшення смуги фільтру ПЧ $B_{пч}$ практично не впливає на результат вимірювання, який наближається до значення:

$$U_{івим} = U_i / q\,, \qquad (3)$$

де U_i – рівень і-тої гармоніки для нескінченної послідовності імпульсів; $U_{івим}$ – виміряне значення гармоніки; q – коефіцієнт шпаруватості пачок. Таким чином, в залежності від встановленого режиму вимірювання, результати вимірювання рівня гармоніки для пачки періодичних імпульсів може змінюватися від дійсного рівня гармоніки U_i у пачці до рівня U_i/q.

Необхідну смугу пропускання $B_{пч}$ в режимі вимірювання середнього значення рівня гармоніки за період U_i/q теж можна визначити експериментально. Критерій для визначення – якщо подальше зменшення смуги $B_{пч}$ не призводить до достатньої зміни рівня виміряної гармоніки.

Недоліком вимірювань з дуже вузькою смугою $B_{пч}$ є збільшення пропорційно $1/B_{пч}$ часу сканування. Наприклад для смуги пропускання $B_{пч}$ = 1 Гц, смуги огляду ΔF = 10 Гц і кількості усереднень n = 10 час вимірювання рівнів амплітуд однієї гармоніки досягає майже 15 хвилин. Тому режим вимірювання з дуже вузькою смугою $B_{пч}$ доцільно використовувати тоді, коли відомі частоти гармонік тестового сигналу, а задачею вимірювання є тільки уточнення їх рівнів.

Для приблизного визначення напруги шумової доріжки аналізатора спектру з вхідним опором 50 Ом для режиму вимірюваня з усередненням можна використовувати формулу [1]:

$$U_{ш0} = -64{,}3 + K_{ш} + 10\lg(B_{ПЧГц}) \text{ [дБ/мкВ]}, \qquad (4)$$

де $Кш$ – коефіцієнт шуму аналізатора спектру в дБ (типове значення 25 дБ); $B_{ПЧГц}$ – значення смуги фільтру ПЧ в Гц. Для режиму з фіксацією максимальних значень до визначеного значення слід додати ще приблизно 12 дБ.

Згідно (4) для смуги $B_{пч}$ = 1 Гц шумова доріжка буде на рівні -32 дБ/мкВ. За умови перевищення рівня сигналу над шумом на 10 дБ можливо вимірювання рівнів гармонік, амплітуда яких перевищує -22 дБ/мкВ. Встановлення смуги $B_{пч}$ = 100 кГц та використання режиму фіксації максимальних значень підвищує рівень шумової доріжки до 26 дБ/мкВ. Різниця в чутливості значна.

Для сигналів побічного електромагнітного випромінювання, рівень яких зазвичай малий в порівнянні з рівнем оточуючого шуму, існує можливість виявлення рівнів гармонік тестового сигналу тільки шляхом зменшення смуги $B_{пч}$ з використанням режиму усереднення результатів багаторазового вимірювання. При цьому значення результату вимірювання буде меншим за дійсне значення амплітуди гармоніки у пачці імпульсів.

Параметр шпаруватості q, а точніше значення поправки q_k, яка враховує зменшення значень виміряного рівня гармоніки $U_{івимk}$ відносно дійсного рівня гармоніки U_i в імпульсі для k-ого значення смуги ПЧ визначається як:

$$q_k = U_i / U_{івимk} \qquad (5)$$

і може бути визначена за результатами вимірювання в лінії, яка є джерелом випромінювання.

В лінії поширюються сигнали достатньо високого рівня (від 0,3 В) і значення рівня перших гармонік завжди можна визначити в режимі фіксації максимальних значень шляхом вимірювання рівня гармонік з достатньо широкою смугою $B_{пч}$. За результатами другого вимірювання з конкретним k-тим значенням смуги $B_{пчk}$ можна виміряти рівень тієї ж гармоніки в лінії $U_{івимk}$ для смуги $B_{пчk}$. Співвідношення між результатами вимірювання рівня гармоніки у лінії і у просторі однакові. Тому можна перерахувати співвідношення виміряного значення гармоніки у просторі $U_{івимk}$ до шуканого значення U_i шляхом вимірювання поправочного коефіцієнту q_k в лінії.

Для вимірювання сигналу в лінії потрібні пробники напруги або струму, розраховані на діапазон частот від 10 кГц до 1-3 ГГц. Підключення таких пристроїв до ліній неможливо без зміни форми і рівня сигналів, що поширюються в лінії. Особливо це стосується вимірювань на частотах вищих за 100 МГц. Наприклад, спеціальні пробники напруги з вхідною ємністю 1 пФ на частоті 300 МГц мають вхідний опір 500 Ом, що суттєво впливає на точність вимірювання рівня гармоніки імпульсних сигналів в лініях з хвильовим опором 50-100 Ом.

Проте параметри пробників або інших пристроїв для під'єднання аналізатора спектру до лінії будуть однаковими для дуже вузької смуги ($\Delta f/f = 10^{-9}…10^{-6}$) і для відносно широкої смуги ($\Delta f/f = 10^{-3}…10^{-2}$) частот, оскільки в нашому сприйнятті «широка» смуга є вузькою в звичайному сприйнятті. Тому вимоги для пристроїв під'єднання спрощуються. Несуттєвим є вплив пристрою на зміну рівня або форми сигналу в лінії за умови, що цей вплив є однаковим для двох вимірювань. Це знімає вимоги щодо їх калібрування.

Використання пробників напруги або вимірювальних трансформаторів струму, що серійно виготовляються в більшості випадків недоцільно для вимірювання сигналів в кабелях сучасних ПЕОМ, оскільки для під'єднання таких пристроїв потрібно порушувати цілісність ізоляції проводів або відокремлювати проводи від цілісної за своєю структурою лінії. Більш зручним є використання окремих відгалужувачів сигналу зі стандартними для цієї лінії роз'ємами.

Тестові сигнали в засобах ЕОТ створюються шляхом передаванням файлів, які крім поля даних у вигляді чергування імпульсів різного рівня (0 та 1 або 1 та-1) мають на початку і в кінці кожного файлу службові дані – ті ж самі сигнали, але різної тривалості. Службові дані впливають на результат вимірювання рівня гармоніки. Розглянемо це питання більш детально.

Файловий тестовий сигнал можна представити у вигляді двох сигналів: поля даних як пачки періодичних імпульсів та службового поля, для якого заздалегідь невідома послідовність двійкових сигналів. Період повторення T обох сигналів однаковий, але вони мають зсув у часі. Спектр двох сигналів – це сума спектрів кожного з урахуванням різниці фаз між гармоніками двох сигналів $-j\omega_i\tau_з$ ($\tau_з$ – зсув послідовностей у часі). В залежності від різниці фаз це може збільшувати і зменшувати середній рівень гармоніки за час його вимірювань. Найбільшим буде вплив, коли службове поле повторює за своєю структурою структуру поля даних. При цьому рівень гармонік спектру на центральних частотах тестового сигналу $\omega_i = 0{,}5i/\tau$ може змінюватися в межах $U_{івим}(1\pm n_с/n_д)$, де $U_{івим}$ – рівень і-тої гармоніки в послідовності з таким же періодом, але без службового поля; $n_с$ та $n_д$ - відповідно кількість символів службового поля та поля даних. Проте вплив службового поля на результати вимірювань буде однаковим, як під час вимірювання рівнів гармоніки у лінії так і у просторі.

В режимі вимірювання з відносно широкою смугою $B_{пч}$ та з фіксацією максимальних значень вплив службового поля можна не враховувати, оскільки за час передавання поля даних рівень сигналу на виході фільтру ПЧ досягне свого максимального значення і це значення фіксується аналізатором спектру. Тому

визначений поправочний коефіцієнт q_k за результатами вимірювання реального тестового файлу у лінії можна використовувати для розрахунку рівня гармоніки U_i у полі.

Для непарних гармонік тестового сигналу вплив службового поля на результати вимірювань рівня гармонік не залежить від номеру гармоніки, оскільки різниця фаз $-j\omega_i\tau_з$, з якою гармоніки службового поля додаються до гармонік поля даних, кратна 2π. При цьому значення поправочного коефіцієнту q_k можна визначати за результатами вимірювань на одній частоті, переважно першої гармоніки тестової послідовності.

У випадку, коли довжина періодичної послідовності у файлі мала і виконати умову $B_{пч} > 3/t_n$ не дозволяють можливості даного аналізатора спектру, рівень першої гармоніки тестового сигналу в лінії приблизно можна розрахувати за формулою

$$U_1 = 0{,}45Ua, \qquad (6)$$

де Ua – амплітуда імпульсу сигналу в лінії. Типове значення і межі відхилень амплітуди імпульсу для кожного інтерфейсу стандартизовані. Якщо інформація передається "симетричними" сигналами і задані рівні зміни напруги у кожному проводі ±Uc, тоді Ua=4Uc.

Вибір першої гармоніки періодичного сигналу пояснюється тим, що на її рівень значно менше вливає форма імпульсу [2]. Наприклад, для прямокутних імпульсів рівень першої гармоніки визначається $U_1 = 0{,}45Ua$, третьої – $U_3 = 0{,}15Ua$. Для імпульсних сигналів у вигляді частин синусоїди перша гармоніка $U_1=0{,}35Ua$, а вищі взагалі відсутні ($U_3 = 0$, $U_5 = 0$).

Розглянемо обмеження щодо доцільності зменшення смуги пропускання фільтру ПЧ під час вимірювання рівня гармонік пачок періодичних імпульсів малої амплітуди. За рахунок зменшення смуги пропускання фільтру ПЧ зменшується рівень шуму аналізатора спектру, але при цьому зменшується у q раз і середній рівень гармоніки. Тому мінімальний рівень гармоніки для такого режиму $U_{1i\min}$ вимірювань за умови перевищення шумової доріжки на 10 дБ відповідно до (4) становить

$$U_{1i\min} = -54{,}3 + K_ш + 10\lg(B_{ПЧ\,1Гц}) + 20\lg(q) \text{ [дБ/мкВ]}, \qquad (7)$$

В режимі вимірювань з фіксацією максимальних значень рівень шумової доріжки збільшується як за рахунок розширення смуги пропускання фільтру ПЧ, так і за рахунок фіксації максимальних значень шуму (на 12,5 дБ). При цьому можна виміряти рівень гармошки в пачці, а не його середнє значення за період. Тому для такого режиму вимірювань чутливість аналізатора спектру можна визначити як:

$$U_{2i\min} = -54{,}3 + K_ш + 10\lg(B_{ПЧ\,2Гц}) \text{ [дБ/мкВ]}. \qquad (8)$$

Мінімальний рівень гармоніки, який можна виміряти, залежить від співвідношення смуг *Впч2/Впч1* та значення шпаруватості тестової послідовності q. Наприклад, для тестового сигналу клавіатури PS/2 довжина пачки $t_n = 0{,}72$ мс, а q = 30. Вимірювання зі смугою *Впч* = 5 кГц в режимі фіксації максимальних значень відповідає вимозі $B_{пч} > 3/t_n$ і дозволяє отримувати прямі результати вимірювань рівня гармоніки. В режимі вимірювань з усередненням результатів для вимірювань гармоніки з меншим рівнем потрібно встановлювати смугу пропускання *Впч1* < 100 Гц, оскільки при значенні *Впч* = 100 Гц розрахунки за формулами (7) та (8) дають практично однакові результати.

Висновки

Вимірювання рівня гармонік аналізатором спектру здійснюється з паузами, які виникають внаслідок сканування з частотою та затримкою на обчислення і індикацією результатів вимірювання. Імпульсний режим вимірювання не впливає на результат вимірювання безперервних сигналів. Для сигналів у вигляді пачок імпульсів результат вимірювань стає залежним від

часу появи пачки і моменту вимірювання рівня гармоніки сигналу.

На результати вимірювання впливає вибрана смуга пропускання фільтру ПЧ $B_{пч}$. Зменшення смуги $B_{пч}$ та усереднення результатів дозволяє збільшити чутливість аналізатора спектру. Проте слід враховувати, що за рахунок зменшення швидкості наростання сигналу у фільтрі ПЧ за час існування пачки амплітуда сигналу не встигає досягнути свого максимального значення.

Поправку, на яку слід збільшити значення результатів вимірювань для розрахунку рівня гармоніки пачки імпульсів, можна визначити за результатами двох вимірювань сигналу у лінії, якою поширюється і при цьому випромінюється цей сигнал. Перше вимірювання здійснюється з достатньо широкою смугою пропускання фільтру ПЧ в режимі фіксації максимальних значень. За декілька циклів сканування наступить момент співпадіння часу приходу пачки імпульсів з часом її вимірювання і результат вимірювання буде визначати рівень гармоніки у пачці імпульсів. Друге вимірювання в лінії здійснюється в режимі усереднення результатів і з такою смугою фільтру ПЧ, як і під час вимірювання рівня слабкого сигналу у просторі.

Вимірювання в лінії потребує додаткових пристроїв для під’єднання входу аналізатора до проводів лінії. При цьому на частотах понад 100 МГц важко забезпечити умови малого спотворення імпульсів під час таких вимірювань. Але за умови незмінності параметрів пристрою під’єднання, його вплив на результати вимірювань рівнів однакових гармонік з відносно широкою і вузькою смугою $B_{пч}$ буде однаковим. Це знімає вимоги щодо калібрування таких пристроїв.

Перелік посилань

[1] К. Раушер, Ф. Йансен, Р. Миналхолд. *Основы спектрального анализа*. М, 2005. 223 с.

[2] Ю. В. Кузнецов, А. Б. Баев. *Спектральный и временной анализ импульсных и периодических сигналов*: *Учебное пособие*. – М.: Изд-во МАИ, 2007. – 95 с.

References

[1] K. Rausher, F. Jansen, R. Minalhold. *Osnovy spektral'nogo analiza*. M, 2005. 223 s.

[2] Ju. V. .Kuznecov, A. B. Baev. *Spektral'nyj i vremennoj analiz impul'snyh i periodicheskih signalov*: *Uchebnoe posobie*. – M.: Izd-vo MAI, 2007. – 95 s.

Реферат

Стеченко Василь; Танцюра Денис

Особливості вимірювання пачок періодичних імпульсних сигналів за допомогою аналізатора спектру

Завдяки зменшенню смуги пропускання фільтру проміжних частот підвищується чутливість аналізатора спектру, що дозволяє виявити гармоніки тестового сигналу з малими рівнями. Параметри тестового сигналу обмежені стандартом прийнятого інтерфейсу передавання даних електронно-обчислювальної техніки.

Для типових аналізаторів спектру при вимірюванні рівнів гармонік періодичних сигналів результати вимірювань стають залежними від параметрів налаштувань аналізатора. Тому є доцільним визначати поправки для перерахунку рівня гармоніки у пачці імпульсів.

Поправку, на яку слід збільшити результати вимірювань для розрахунку рівня гармоніки для пачки імпульсів, можна визначити за результатами двох вимірювань сигналу у лінії, якою поширюється і випромінюється цей сигнал.

Вимірювання в лінії потребує додаткових пристроїв для під’єднання входу аналізатора до проводів лінії. При цьому на частотах понад 100 МГц важко виконати умови малого спотворення імпульсів під час таких вимірювань. Але за умови незмінності параметрів пристрою під’єднання, вплив пристрою на результати вимірювань рівнів однакових гармонік з відносно широкою і вузькою смугою буде однаковим. Тому зникають вимоги щодо калібрування таких пристроїв.

Стеченко Василий; Танцюра Денис

Особенности измерения пачек периодических импульсных сигналов с помощью анализатора спектра

Благодаря уменьшению полосы фильтра промежуточных частот повышается чувствительность анализатора спектра, что позволяет выявить гармоники тестового сигнала с малой амплитудой. Параметры тестового сигнала ограничены стандартом принятого интерфейса передачи данных электронно-вычислительной техники.

Для типичных анализаторов спектра при измерении уровня гармоник периодических сигналов результаты измерений становятся зависимыми от параметров настройки анализатора. Поэтому целесообразно определять поправки для пересчета уровня гармоники в пачке импульсов.

Поправку, на которую нужно увеличить результаты измерения для расчета уровня гармоники для пачки импульсов, можно определить по результатам двух измерений сигнала в линии, которой распространяется и излучается этот сигнал.

Измерения в линии требует дополнительных устройств для подключения входа анализатора к проводам линии. При этом на частотах свыше 100 МГц трудно выполнить условия малого искажения импульсов при таких измерений. Но при условии неизменности параметров устройства подключения, влияние устройства на результаты измерения уровней одинаковых гармоник с относительно широкой и узкой полосой будет одинаковым. Поэтому исчезают требования по калибровке таких устройств.

Stechenko Vasil; Tantsyura Denis

Features of measuring the layer of periodic pulse signals by the spectra analyzer

By reducing the band of analysis, the sensitivity of the spectrum analyzer increases, which allows to detect the harmonics of the test signal. Parameters of the test signal are limited by the standard adopted by the data interface.

For typical spectrum analyzers when measuring the harmonics of periodic signals, the results of measurements become dependent on the parameters of the analyzer's settings. Therefore, it is expedient to determine the corrections to convert the harmonic level into a packet of pulses.

It is shown that the correction, on which it is necessary to increase the results of measurement to calculate the harmonic level for a pulse packet, can be determined by the results of two measured signals in the line to which this signal propagates and emits.

Measurement in the line requires additional devices to connect the analyzer's input to the line wires. At the same time, at the frequencies above 100 MHz it is difficult to fulfill the conditions for small distortion of the pulses during such measurements. But provided the parameters of the connection device are unchanged, the effect of the device on the results of measurement of identical harmonics with a relatively wide and narrow band will be the same. Therefore, the requirements for calibrating such devices disappear.

Відомості про авторів

Стеченко Василь Митрофанович
Освіта: Вища, спеціальність "Радіоінженер" (1972).
Науковий ступінь: Кандидат технічних наук (1980).
Місце роботи: Науково-дослідний центр систем технічного захисту інформації "ТЕЗІС" Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського".
Email: *v.stechenko@kpi.ua*

Танцюра Денис Васильович
Освіта: Вища, спеціальність "Магістр електронних апаратів" (2008).
Місце роботи: Науково-дослідний центр систем технічного захисту інформації "ТЕЗІС" Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського".
Email: *tantsyura@kivra.kpi.ua*

5. Підготовка та підвищення кваліфікації спеціалістів систем захисту інформації

УДК 681.3.06

МЕТОДИЧНІ ОСОБЛИВОСТІ ВИВЧЕННЯ ПОНЯТТЯ І ОБЧИСЛЕННЯ ПАРАМЕТРІВ ТЕОРЕТИЧНОЇ СЕКРЕТНОСТІ В КОМП'ЮТЕРНІЙ КРИПТОГРАФІЇ

Сапсай Тетяна; Тарасенко Володимир; Тесленко Олександр
КПІ ім. Ігоря Сікорського

METHODICAL FEATURES FOR STUDY OF CONCEPT AND PARAMETERS CALCULATION OF THEORETICAL SECRECY IN COMPUTER CRYPTOGRAPHY

Sapsai Tetiana; Tarassenko Volodymyr; Teslenko Oleksandr
Igor Sikorsky Kyiv Polytechnic Institute

Анотація: **Розглянуто методичні особливості обчислення апостеріорних ймовірностей початкових повідомлень та ключів і визначення базових властивостей криптографічних перетворень.**
Ключові слова: **Криптографічні перетворення, теоретична секретність, обчислення.**
Summary: **Methodical features of calculation for an aposteriori probability of initial messages and keys and determination of the basic properties cryptographic transformations.**
Key words: **Cryptographic transformations, theoretical secrecy, calculation.**

Вступ

Як результат швидкого розвитку і масового впровадження комп'ютерних мережевих технологій наразі обов'язковою частиною їх системного програмного забезпечення стали засоби криптографічних перетворень. Користувачі комп'ютерних систем і мереж можуть застосовувати електронний цифровий підпис, шифрування та розшифрування даних фактично без глибоких знань в області криптографії. Однак, в процесі підготовки фахівців (бакалаврів, магістрів) з комп'ютерної інженерії необхідні, принаймні, базові знання про криптографічні перетворення. Одним із базових понять криптографії є поняття теоретичної секретності, яке визначене Клодом Шенноном [1]. Тому виникає задача створення доступної для комп'ютерної інженерії, але, водночас, достатньо точної послідовності вивчення поняття теоретичної секретності та відповідних властивостей симетричних криптографічних комп'ютерних перетворень.

Визначення властивостей симетричних криптографічних перетворень

Відповідно до [1] розглянемо секретну систему, яка включає множину M початкових повідомлень, множину K ключів та множину E криптограм. Особливістю комп'ютерної криптографії є те, що $M, K, E \subset V^*$, де V^* – множина скінчених послідовностей з 0 та 1. Не порушуючи загальності викладу, будемо вважати, що всі елементи множини M мають однакову довжину. Аналогічно вважаємо це і для множин K та E. Введемо наступні позначення: малими буквами латинського алфавіту m, k та e будемо позначать **змінні,** які приймають значення з відповідних множин. Цими ж буквами, але із індексами, будемо позначати конкретні елементи множин, наприклад, $m_i \in M$, $i = 1, 2, \left|M\right|$, $k_j \in K$, $j = 1, 2, \ldots, \left|K\right|$, $e_s \in E$, $s = 1, 2, \ldots, \left|E\right|$. ($\left|X\right|$ –

кількість елементів множини X). Шляхом декартового добутку утворимо множину $D = M \cdot K \cdot E$. Кожний елемент множини D є кортеж (впорядкована послідовність) $< m_i, k_j, e_s >$. Позначимо як F довільну підмножину множини D (тернарне відношення) $(F \subset D)$. Будь-яке відношення F визначає наступну функцію:

$$\varphi(m,k,e) = \begin{cases} 1, якщо < m,k,e > \in F, \\ 0, якщо < m,k,e > \in \overline{F} \end{cases}$$

Секретна система Шеннона фактично включає криптографічне перетворення R, як тернарне відношення на множині D. Криптографічне перетворення R визначає пряме криптографічне перетворення (шифрування) – одержання e на основі m та k, а також обернене криптографічне перетворення (розшифрування) – одержання m на основі e та k [1]. Зауважимо, що криптографічне перетворення R визначає і таке криптоаналітичне перетворення – одержання k на основі m та e. Очевидно, що далеко не всі можливі тернарні відношення F можуть бути використані як криптографічні перетворення. Тому виникає необхідність визначення властивостей криптографічних перетворень R.

Виходячи з міркувань практичної застосовності R поставимо до нього наступні вимоги:

1) Для будь-яких $m_i \in M$ та $k_j \in K$ повинно існувати тільки одне $e_s \in E$ таке, що $\varphi(m_i, k_j, e_s) = 1$. Іншими словами, будь-яке початкове повідомлення може бути зашифровано будь-яким ключем. При цьому формується одна і тільки одна криптограма.

2) Для будь-яких $e_s \in E$ та $k_j \in K$ може існувати тільки одне $m_i \in M$, таке, що $\varphi(m_i, k_j, e_s) = 1$. Інакше, за одержаною від попереднього шифрування криптограмою при заданому ключі розшифрування має бути однозначним.

Очевидно, що перша вимога обґрунтовує існування всюди однозначно визначеної функції шифрування $e = f(m,k)$, яка може бути подана таблицею, наприклад, табл.1 .

Таблиця 1.

	m_1	m_2
k_1	e_1	e_3
k_2	e_1	e_2
k_3	e_2	e_3

Відповідно до першої умови будь-яка клітинка такої таблиці не може бути пустою і не може мати більше ніж одну криптограму. Тут і далі будемо вважати, що стовпчики таблиці позначаються початковими повідомленнями, а рядки – ключами.

Друга умова обґрунтовує існування функції розшифрування $m = f^1(e,k)$, яка також може бути задана таблицею (табл. 2)

Таблиця 2.

	e_1	e_2	e_3
k_1	m_1	-	m_2
k_2	m_1	m_2	m_2
k_3	-	m_1	-

Відповідно до другої умови в будь-якій клітинці такої таблиці не може бути більше ніж одне початкове повідомлення. У загальному випадку функція розшифрування може бути не визначеною на деяких значеннях аргументів, тобто функція розшифрування може бути частково визначеною функцією.

Важливим наслідком другої умови є те, що в будь-якому рядку таблиці функції шифрування (табл.1) усі криптограми різні, тобто для будь-яких m_{i1}, m_{i2}, таких, що $m_{i1} \neq m_{i2}$ та будь-якого ключа k маємо $f(m_{i1}, k) \neq f(m_{i2}, k)$. Звідси випливає наступне співвідношення між кількістю початкових повідомлень та криптограм – $|M| \leq |E|$, тобто кількість криптограм не може бути меншою за кількість початкових повідомлень.

Зауважимо, що виконання вимог 1) і 2) не гарантує існування однозначно визначеної криптоаналітичної функції, тобто в загальному випадку значення ключа при заданих m та e не завжди визначається однозначно. Дійсно, в розглянутому прикладі маємо наступне криптоаналітичне перетворення (табл. 3).

Таблиця 3.

	e_1	e_2	e_3
m_1	k_1,k_2	k_3	-
m_2	-	k_2	k_2,k_3

Шеннон визначив поняття теоретичної секретності, яке полягає в наступному. Нехай криптоаналітику (противнику) доступні функції шифрування та розшифрування, нехай противник володіє необмеженими обчислювальними можливостями та має необмежений час для обчислень. Секретна система, яка включає множини $M, K, E,$ функцію $e = f(m,k)$ та функцію $m = f^1(e,k)$ є теоретично секретною, якщо, не знаючи ключа k, криптоаналітик, перехопивши криптограму e_s, не одержить ні одного біта інформації про початкове повідомлення. Враховуючи наявність в криптоаналітика безмежного часу та безмежних обчислювальних можливостей, теоретична секретність фактично означає, що алгоритм атаки на початкове повідомлення взагалі не існує. Згідно із Шенноном теоретична секретність досягається тоді і тільки тоді, коли апостеріорні ймовірності початкових повідомлень співпадають з їх апріорними ймовірностями. Під апріорними ймовірностями мають на увазі ймовірності початкових повідомлень (позначимо $P(m_i)$) та ключів (позначимо $P(k_j)$) до перехоплення криптограми. Апріорні значення ймовірностей початкових повідомлень криптоаналітик може встановити на свій розсуд на основі відомостей про джерело повідомлень. При цьому вважається, що $P(m_i) \neq 0$ для всіх значень i, оскільки в іншому випадку фактично зменшується кількість початкових повідомлень.

Апріорі криптоаналітик вимушений вважати, що користувач секретної системи забезпечив рівноймовірність ключів. Апостеріорна ймовірність початкового повідомлення m_i (позначимо $Pe_s(m_i)$) – це ймовірність цього повідомлення, обчислена після перехоплення криптограми e_s. Криптаналітик може довільно вгадувати, що було передано, але у випадку забезпечення теоретичної секретності після перехоплення криптограми в нього не буде жодних підстав для розвитку чи поглиблення своїх догадок.

Оскільки початкове повідомлення і ключ вибираються незалежно один від одного, то для обчислення апостеріорних ймовірностей початкових повідомлень після перехоплення криптограми e_s використовують формулу Байєса [2]:

$$Pe_s(m_i) = \frac{P(m_i) \times Pm_i(e_s)}{P(e_s)},$$

де $Pm_i(e_s)$ – ймовірність криптограми e_s за умови, що шифрували повідомлення m_i, а $P(e_s)$ – ймовірність появи криптограми e_s при шифруванні будь-яких початкових повідомлень.

Із рівності $Pe_s(m_i) = P(m_i)$ випливає необхідність виконання рівності $Pm_i(e_s) = P(e_s)$, тобто ймовірність появи криптограми e_s при шифруванні конкретного початкового повідомлення дорівнює ймовірності її появи взагалі.

Значення $Pm_i(e_s)$ обчислюємо за наступною формулою:

$$Pm_i(e_s) = \sum_{j=1}^{|K|} P(k_j) \cdot \varphi(m_i, k_j, e_s). \qquad (1)$$

Із формули (1) випливає, що значення $Pm_i(e_s)$ дорівнює сумі апріорних ймовірностей ключів, які перетворюють початкове повідомлення m_i в криптограму e_s. Якщо всі ключі рівноймовірні, то

ймовірність будь якого ключа дорівнює $1/|K|$. Нехай $Nm_i(e_s)$ – кількість ключів, які перетворюють початкове повідомлення m_i в криптограму e_s, тобто $Nm_i(e_s)$ – кількість криптограм e_s в стовпчику таблиці шифрування, яка позначена початковим повідомленням m_i. Тоді $Pm_i(e_s) = Nm_i(e_s)/|K|$.

Значення $P(e_s)$ обчислимо за наступною формулою:

$$P(e_s) = \sum_{i=1}^{|M|}\sum_{j=1}^{|K|} P(k_j)\cdot P(m_i)\cdot \varphi(m_i, k_j, e_s).$$

Враховуючи, що Pm_i не залежить від j (вибір початкового повідомлення не залежить від вибору ключа) маємо:

$$P(e_s) = \sum_{i=1}^{|M|}\sum_{j=1}^{|K|} P(k_j)\cdot P(m_i)\cdot \varphi(m_i, k_j, e_s),$$

або

$$P(e_s) = \sum_{i=1}^{|M|} P(m_i)\cdot \frac{Nm_i(e_s)}{|K|}.$$

Якщо значення $Nm_i(e_s)$ не залежить від m_i, то $Pm_i(e_s) = Nm_i(e_s)/|K|$, тобто $P(e_s) = Pm_i(e_s)$.

Таким чином, **достатньою** умовою досягнення рівності апостеріорних ймовірностей початкових повідомлень при перехопленні криптограми e_s їх апріорним ймовірностям (тобто, $Pe_s(m_i) = Pm_i$) є незалежність $Nm_i(e_s)$ від m_i для всіх криптограм e_s, $s = 1, 2, \ldots, |E|$. З точки зору вимог до властивостей криптографічних перетворень R це означає, що будь-яка одна і таж конкретна криптограма повинна міститись в кожному стовпчику таблиці функції шифрування однакову і не нульову кількість разів. Різні криптограми можуть міститись в стовпчиках таблиці різну (але не нульову) кількість разів. Іншими словами, при прямому криптографічному перетворенні будь-якого початкового повідомлення всіма ключами конкретна криптограма повинна створюватись однакову (не нульову) кількість разів. Математично це можна сформулювати наступним чином: для будь-яких криптограм e_s та будь-яких початкових повідомлень m_{i1}, m_{i2}, таких, що $m_{i1} \neq m_{i2}$ справедлива рівність

$$\sum_{j=1}^{|K|}\varphi(m_{i1}, k_j, e_s) = \sum_{j=1}^{|K|}\varphi(m_{i2}, k_j, e_s) \neq 0. \qquad (2)$$

Із рівності (2) випливає, що кількість ключів не може бути меншою за кількість криптограм, тобто $|E| \le |K|$, або відповідно до попереднього, маємо

$$|M| \le |E| \le |K|.$$

Аналогічно викладеному, можна обчислити апостеріорні ймовірності ключів, де $Pe_s(k_j)$ – апостеріорна ймовірність ключа kj при перехопленні криптограми e_s, тобто

$$Pe_s(k_j) = \frac{P(k_j)\times Pk_j(e_s)}{P(e_s)},$$

де $P(k_j) = 1/|K|$ – апріорні ймовірності ключів, $Pk_j(e_s)$ – ймовірність криптограми e_s за умови, що для шифрування будь-якого початкового повідомлення використовувався ключ kj, $P(e_s)$ – ймовірність криптограми e_s за умови, що для шифрування будь-якого початкового повідомлення використовувався будь-який ключ.

Значення $Pk_j(e_s)$ дорівнює сумі апріорних ймовірностей початкових повідомлень, які перетворюються в криптограму e_s при використанні ключа kj

$$Pk_j(e_s) = \sum_{i=1}^{|M|} P(m_i)\cdot \varphi(m_i, k_j, e_s).$$

Якщо кількість початкових повідомлень дорівнює кількості криптограм, тобто $|M| = |E|$, то внаслідок необхідності забезпечення однозначного розшифрування

завжди буде існувати одне і лише одне початкове повідомлення (m_x), $x \in \{1,2,\ldots|M|\}$ таке, що $\varphi(m_x, k_j, e_s) = 1$, а $\varphi(m_i, k_j, e_s) = 0$, $(i \neq x)$. Звідси випливає, що $Pk_j(e_s) = P(m_x)$, тобто апостеріорні ймовірності ключів дорівнюють апріорним ймовірностям відповідних початкових повідомлень.

Якщо $|M| \leq |E|$, то для будь-якого ключа kj будуть існувати такі $y \in \{1,2,\ldots,|E|\}$, що $\varphi(m_i, k_j, e_y) = 0$ при всіх $i = 1,2,\ldots,|M|$, тобто $Pk_j(e_y) = 0$. Для інших криптограм, які у випадку $|M| = |E|$, $Pk_j(e_s) = P(m_x)$.

Зауважимо, що значення $Pk_j(e_s)$ ніяк не залежить від кількості ключів, звідки випливає, що при $|M| = |E|$ криптоаналітик не зможе отримати жодного біта інформації про ключ навіть коли $|K| < |M|$.

Розглянемо окремі випадки, обумовлені різними співвідношеннями кількості елементів в множинах M, K, E.

Нехай $|M| = |E| = |K|$. У цьому випадку таблиця функції шифрування є так званим латинським квадратом, в якому будь-який рядок і будь-який стовпчик не мають однакових криптограм.

При $|M| = |E| = |K| = 4$ існує 320 латинських квадратів, один із них подано в табл. 4.

Таблиця 4.

	m_1	m_2	m_3	m_4
k_1	e_1	e_2	e_3	e_4
k_2	e_2	e_3	e_4	e_1
k_3	e_3	e_4	e_1	e_2
k_4	e_4	e_1	e_2	e_3

Із табл. 4 слідує, що при перехопленні будь-якої криптограми, наприклад e_2, криптоаналітик не в змозі одержати хоч якусь інформацію про початкове повідомлення та ключ шифрування, оскільки криптограма e_2 (як і інші криптограми) рівномірно розподілена серед стовпчиків та рядків таблиці.

Нехай $|M| = |E| = |K| / N$, в цьому випадку кожний стовпчик таблиці функції шифрування має рівно N кожної криптограми (нагадаємо, що будь-який рядок згідно із другої умови не може мати однакових криптограм). Таку таблицю назвемо латинським прямокутником. Фактично латинський прямокутник складається з N латинських квадратів, які попарно не мають однакових рядків. У табл. 5 подано приклад функції шифрування при $|M| = |E| = |K| = 8$.

Таблиця 5.

	m_1	m_2	m_3	m_4
k_1	e_1	e_2	e_3	e_4
k_2	e_2	e_3	e_4	e_1
k_3	e_3	e_4	e_1	e_2
k_4	e_4	e_1	e_2	e_3
k_5	e_1	e_3	e_4	e_2
k_6	e_3	e_4	e_2	e_1
k_7	e_2	e_1	e_3	e_4
k_8	e_4	e_2	e_1	e_3

Як і раніше, при перехопленні будь-якої криптограми, наприклад e_2, криптоаналітик не в змозі одержати хоч яку-небудь інформацію про початкове повідомлення та ключ шифрування.

Зауважимо, що при $|M| = |E|$ будь-який рядок таблиці є деякою перестановкою елементів множини криптограм. Загальна кількість перестановок – $|E|!$. Тому можлива функція шифрування, яка містить усі перестановки елементів множини криптограм, наприклад для $|M| = |E| = 3$ $|K| = 3! = 6$.

Із табл. 6 також слідує, що при перехопленні будь-якої криптограми, наприклад e_2, криптоаналітик не в змозі одержати хоч яку-небудь інформацію про початкове повідомлення та ключ шифрування.

Таблиця 6.

	m_1	m_2	m_3
k_1	e_1	e_2	e_3
k_2	e_1	e_3	e_2
k_3	e_2	e_1	e_3
k_4	e_2	e_3	e_1
k_5	e_3	e_2	e_1
k_6	e_3	e_1	e_2

Функцію шифрування, яка містить усі перестановки криптограм, будемо називати функцією шифрування з повною системою перестановок. Очевидно, що така функція з точністю до позначення ключів тільки одна і будь-яка інша функція шифрування з тими самими значеннями $|M|$ та $|E|$ може бути одержана із цієї функції шляхом зменшення кількості ключів (шляхом видалення відповідних рядків таблиці).

У комп'ютерній інженерії прийнято оперувати не кількістю елементів, а мінімально можливою кількістю двійкових розрядів (довжиною), необхідних для подання елементів, наприклад, $lx = \rceil \log_2 |X| [$, де $\rceil u [$ – найближче більше ціле від u. Тому співвідношення $|M| \le |E| \le |K|$ можна подати наступним чином $l_M \le l_E \le l_K$, тобто довжина криптограми та ключа не може бути меншою за довжину початкового повідомлення.

Наведені вище дані обґрунтовують загальновідоме правило – секретна система, в якій довжина ключа менша за довжину початкового повідомлення не має теоретичної секретності при яких завгодно функціях шифрування.

Підсумовуючи вищевикладене стверджуємо, що теоретична секретність може бути досягнута якщо:

1. $|M| \le |E| \le |K|$ або $l_M \le l_E \le l_K$.

2. Для будь-яких криптограм $e_s \in E$ та початкових повідомлень m_{i1} і m_{i2} $(m_{i1}, m_{i2} \in M)$ справедлива рівність:

$$\sum_{j=1}^{|K|} \varphi(m_{i_1}, k_j, e_s) = \sum_{j=1}^{|K|} \varphi(m_{i_2}, k_j, e_s).$$

3. Для кожного сеансу шифрування ключ має бути одноразовий.

4. Для кожного сеансу шифрування всі ключі рівноймовірні.

Таким чином, для того щоб відношення F можна використовувати як криптографічне відношення R, достатньо виконання умов за висновками 1 і 2. Виконання вимог за висновками 3 і 4 в практиці застосування криптографічних перетворень є значною організаційною та технічною проблемою. Тому, як правило, особливо для захисту конфіденційної інформації використовують дещо простіші вирішення проблеми ключів – потокове та блочне криптографічне перетворення. При потоковому криптографічному перетворенні для генерації ключів як при шифруванні, так і при розшифруванні використовують програмні генератори випадкових чисел. Генератори характеризуються початковим станом із множини початкових станів, алгоритмом функціонування та довжиною без повторності ключів. Вимогою до таких генераторів є неможливість для криптоаналітика передбачити появу чергового ключа з імовірністю, яка відрізняється від $1/|K|$ за умови, що йому відомий алгоритм генератора, відома деяка частина попередніх ключів, але невідомий початковий стан.

У блочних криптографічних перетвореннях початкові дані розбиваються на блоки рівної довжини. Типові значення довжини блоку в сучасних блочних алгоритмах симетричних криптографічних перетворень від 64 до 512 біт. Усі блоки шифрують (або розшифровують) одним ключем. Це значно спрощує технічні засоби та організаційні заходи для генерації, збереження та поширення секретних ключів. Ясно, що теоретична секретність забезпечується лише для одноразового повідомлення довжиною в один блок. Необхідно зауважити, що в практичному використанні алгоритмів блочних симетричних криптографічних перетворень майже завжди, в межах блоку,

кількість початкових повідомлень менша за кількість криптограм, тобто $|M| < |E|$. Оскільки виконується умова висновку 2, то теоретична секретність в межах блоку і в цьому випадку має місце.

Висновки

Запропоновані методичні особливості визначення базових властивостей криптографічних перетворень, які задовольняють вимогам теоретичної секретності та визначення апостеріорних ймовірностей початкових повідомлень, можуть бути використані викладачами ВНЗ при підготовці методичних матеріалів для лабораторних та контрольних робіт з дисциплін «Захист інформації» та «Комп'ютерна криптографія» спеціальності «Комп'ютерна інженерія». Наведені матеріали апробовані при викладанні дисципліни «Комп'ютерна криптографія» на кафедрі системного програмування та спеціалізованих комп'ютерних систем НТУУ «Київський політехнічний інститут імені Ігоря Сікорського»

Перелік посилань

[1] К. Шеннон, *Работы по теории информации и кибернетике.* /Пер. с англ. под ред. Н. А. Железнова. М.: ИЛ, 1963. 829 с.

[2] *Вероятность и математическая статистика.* Энциклопедия /Под ред. Ю.В. Прохорова. М.: БРЭ, 1999. 910с.

References

[1] K. Shennon, *Rabotu po teoryy ynformatsyy y kybernetyke*. /Per. s anhl. pod red. N. A. Zheleznova. M.: YL, 1963. 829 s.

[2] *Veroiatnost y matematycheskaia statystyka.* Эntsyklopedyia /Pod red. Yu.V. Prokhorova. M.: BRЭ, 1999. 910s.

Реферат

Сапсай Тетяна; Тарасенко Володимир; Тесленко Олександр

Методичні особливості вивчення поняття і обчислення параметрів теоретичної секретності в комп'ютерній криптографії

У роботі представлена оригінальна інтерпретація частини ідей Шеннона щодо поняття теоретичної секретності стосовно симетричних криптографічних перетворень в комп'ютерній криптографії та обчислення апостеріорних ймовірностей початкових повідомлень та ключів. Використано подання симетричного криптографічного перетворення як відношення на множині кортежів із початкових повідомлень, ключів та криптограм, яка утворюється шляхом декартового добутку із відповідних множин скінчених послідовностей з 0 та 1. Виходячи з міркувань практичної застосовності та забезпечення теоретичної секретності визначено властивості такого відношення. Наведена методика обчислень легко може бути запрограмована на поширених мовах програмування. Одержані результати дозволяють спростити процес освоєння відповідних теоретичних положень та можуть бути використані при підготовці методичних матеріалів для вивчення основ комп'ютерної криптографії.

Сапсай Татьяна; Тарасенко Владимир; Тесленко Александр

Методические особенности изучения понятия и вычисления параметров теоретической секретности в компьютерной криптографии

В работе представлена оригинальная интерпретация части идей Шеннона относящаяся к понятию теоретической секретности относительно симметричных криптографических преобразований в компьютерной криптографии и вычислений апостериорных вероятностей начальных сообщений и ключей. Использовано представление симметрического криптографического преобразования как отношение на множестве кортежей из начальных

сообщений, ключей и криптограмм, которое образуется путем декартового произведения соответствующих множеств конечных последовательностей 0 и 1. Исходя из соображений практического использования и обеспечения теоретической секретности определено свойства такого соотношения. Приведенная методика вычисления легко может быть запрограммирована с использованием широко известных языков программирования. Полученные результаты позволяют упростить процесс изучения соответствующих теоретических положений и могут быть использованы при подготовке методических материалов для изложения основ компьютерной криптографии.

Sapsai Tetiana; Tarassenko Volodymyr; Teslenko Oleksandr

Methodical features for study of concept and parameters calculation of theoretical secrecy in computer cryptography

The paper presents an original interpretation of the Shannon's ideas related to the concept of privacy with respect to the theoretical symmetric cryptographic transformations in computer cryptography and computation of posterior probabilities of the initial messages and keys. Used representation of symmetric cryptographic transformation as a relation on the set of tuples of the initial messages, keys and cryptograms, which is formed by the Cartesian product of the corresponding sets of finite sequences of 0 and 1. For reasons of practical use and providing a theoretical secrecy defined properties of such relation. The above calculation method can easily be programmed using well-known programming languages. The results help to simplify the process of studying relevant theoretical positions and can be used in the preparation of teaching materials for the presentation of the fundamentals of computer cryptography.

Відомості про авторів

Сапсай Тетяна Григорівна
Освіта: Повна вища, Електронні обчислювальні машини.
Науковий ступінь: Кандидат технічних наук (1992).
Вчене звання: Доцент.
Місце роботи: Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського».
Область знань: Обчислювальна техніка.
Наукові інтереси: Комп‘ютерні компоненти і апаратна реалізація спеціалізованих комп’ютерних систем.
Email: *stg@scs.ntu-kpi.kiev.ua*

Тарасенко Володимир Петрович
Освіта: Повна вища, Автоматики і електроприладобудування.
Науковий ступінь: Доктор технічних наук (1987).
Вчене звання: Професор.
Місце роботи: Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського».
Область знань: Обчислювальна техніка
Наукові інтереси: Комп‘ютерні системи і компоненти.
Email: *vtarasen@scs.ntu-kpi.kiev.ua*

Тесленко Олександр Кирилович
Освіта: Повна вища, Електронні обчислювальні машини.
Науковий ступінь: Кандидат технічних наук (1976).
Вчене звання: Старший науковий співробітник.
Місце роботи: Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського».
Область знань: Комп’ютерна інженерія.
Наукові інтереси: Оптимізація програмних та апаратних реалізацій спеціалізованих комп’ютерних систем.
Email: *teslenko@scs.ntu-kpi.kiev.ua*

АЛФАВІТНИЙ ПОКАЖЧИК

ALPHABETIC INDEX

УДК 638.235.231

ВИМОГИ АВТОРАМ, ЩОДО ОФОРМЛЕННЯ ТЕКСТІВ СТАТЕЙ ДЛЯ ПУБЛІКАЦІЇ У ЗБІРНИКУ «ПРАВОВЕ, НОРМАТИВНЕ ТА МЕТРОЛОГІЧНЕ ЗАБЕЗПЕЧЕННЯ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ В УКРАЇНІ»

Кулій Ростислав[1]; Степаненко Олександр[2]
[1]НДЦ «ТЕЗІС» КПІ ім. Ігоря Сікорського;
[2]Національний авіаційний університет

REQUIREMENTS TO AUTHOR FOR REGISTRATION TEXT ARTICLES REQUIRED THE PUBLICATION "LEGAL, REGULATORY AND METROLOGICAL SUPPORT OF INFORMATION SECURITY SYSTEM IN UKRAINE"

Kulii Rostislav[1]; Stepanov Oleksandr[2]
[1]SRC «TESIS» Igor Sikorsky Kyiv Polytechnic Institute;
[2]National Aviation University

Анотація: **Наведені рекомендації редакції щодо оформлення тексту статей.**
Ключові слова: **Інформація, інформаційна безпека.**
Summary: **Recommendations of edition rather registrations texts of clauses are resulted.**
Keywords: **Information, information security.**

Вступ

Шановні автори, при підготовці публікацій у збірнику "Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні" дотримуйтесь цих правил оформлення матеріалів статей (електронну версію вимог шукайте на сайті збірника http://pnzzi.kpi.ua/Docs/vymogystat.doc).

Вимоги до документу

Рукописи статей оформлюються однією з трьох мов – українською, російською, англійською.

Налаштування сторінки документу наведено в табл. 1. Формат документів: *.doc/*.docx, орієнтовно 4 – 8 повних сторінок.

Таблиця 1.

Вимоги до налаштувань сторінки

Налаштування сторінки	
Формат сторінки	А4 (210х297мм)
Верхнє поле	25 мм
Нижнє поле	25 мм
Ліве поле	22,5 мм
Праве поле	22,5 мм

Тексти статей мають бути набрані в текстовому редакторі Microsoft Word 2003 і вище (або у сумісному текстовому редакторі), шрифт Times New Roman, інтервал – одинарний.

Правила оформлення та порядок тексту повинні бути такі:

– індекс УДК (верхній лівий кут, без абзацу, 12 пт, напівжирний, інтервал після рядка 14 пт);

– назва статті (в центрі, великими літерами, 14 пт, напівжирний, інтервал після рядка 14 пт);

– прізвище та ім’я автора(ів) (в центрі, 12 пт, напівжирний, курсив);

– місце роботи (в центрі, 10 пт, курсив);

– назва статті англійською мовою (в центрі, великими літерами, 12 пт, напівжирний, інтервал перед рядком 14 пт);

– прізвище та ім’я автора(ів) англійською мовою (в центрі, 12 пт, напівжирний курсив);

– місце роботи англійською мовою (в центрі, 10 пт, курсив, інтервал після рядка 14 пт);

– анотація і ключові слова українською та англійською мовами (відступ від лівого поля 20мм, 10 пт (див. приклад вище));

– заголовки розділів в окремому рядку тексту (в центрі, 12 пт, напівжирний, інтервал перед і після рядка 6 пт);

– текст статті (12 пт, абзац 5 мм, вирівнювання по ширині, в дві колонки, шириною 80мм, розділ між колонками 5 мм);

– перелік посилань (10 пт, вирівнювання по ширині (див. приклад нижче)) слідує за текстом статті і, за можливості, супроводжується адресами на джерела в Інтернет;

– "References" (10 пт, вирівнювання по ширині (див. приклад нижче)) для перетворення кирилиці в романський алфавіт слід використовувати системи автоматичної транслітерації. Рекомендуємо використовувати ресурс: http://www.translit.kh.ua/ з настройками **«Паспортний КМУ 2010»**;

– реферати статті (українською, російською та англійською мовами 45 – 50 рядків кожен) має мати структуру: прізвище та ім'я автора(ів), назва статті, текст реферату (див. приклад нижче));

– відомості про автора.

Формули та позначення набирати у редакторі формул MathType 5 і вище, як окремий об'єкт з розмірами: змінна – 12 пт, великий індекс – 7 пт, малий індекс – 5 пт, великий символ – 16 пт, малий символ – 10 пт; кирилиця, грецька та цифри - прямі, латиниця – курсив. Розміщення формули — по центру, нумерації — по правому краю, згідно прикладу представлення формули (1). Великі формули повинні бути розбиті на декілька рядків. Ширина формули не повинна виходити за границі тексту.

$$s(t) = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \left\{ a_k \cos\left[2\pi \left(f_0 + \frac{k}{T} \right) t \right] \right\} \qquad (1)$$

Таблиці не повинні виходити за межі тексту. Вони можуть мати заголовок, розміщений над самою таблицею (в центрі, 12 пт, напівжирний). Текст таблиці 12 пт. Нумерацію таблиці слід вирівняти по правому краю (приклад у табл. 1).

Рисунки слід розміщувати в таблиці з властивостями: границі не відображаються, вирівнювання по центру (див. рис. 1).

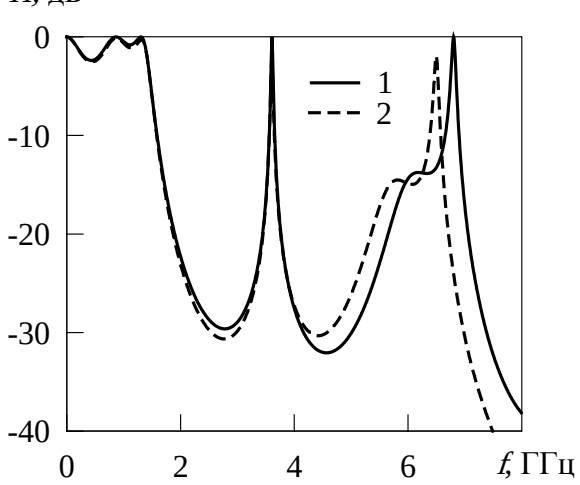


Рис. 1 – Приклад оформлення рисунків

Всі зображення в документі повинні бути у форматі *.png або *.jpeg з якістю, достатньою для друку (не менше **300**dpi). Рисунок має бути згрупованим об'єктом з написами і шкалами графіків, які при зменшенні масштабу в 2 – 3 рази відповідають шрифту 10 пт. Рисунки, які мають позиції *а*, *б*, …, повинні бути однакової висоти і скомпоновані по горизонталі. Мінімальна товщина ліній 0,5 пт. Кожний рисунок має бути підписаний знизу (Times New Roman, 12 пт, в центрі, інтервал до та після підпису під рисунком 6 пт).

Обов'язкове посилання в тексті статі на кожний рисунок. Розміщувати рисунки необхідно поряд або після посилання на нього. Позначення при посиланні на формулу – (1), (1, 2); рисунок – рис. 1, рис. 1, 2; таблицю – табл. 1, табл. 1, 2; літературне джерело – [1]; [1], [2]; [1] – [3].

Кількість таблиць та рисунків, що містяться в тексті статті має бути мінімально необхідною і не перевищувати половини кількості сторінок тексту статті.

Висновки

Рукопис оформлений відповідно до цих вимог слід надсилати на Email редакції. Після цього до Вас на Ваш Email прийде підтвердження отримання рукопису. Далі редактор виконає формальну перевірку рукопису на відповідність вимогам до оформлення статей та направить його на рецензування. Матеріали, що оформлені з відхиленнями від встановлених вимог, направляються авторам на доопрацювання. У разі виникнення запитань звертайтесь за тел. +380442048385 або Email (**pnzzi@tesis.kiev.ua**) до редакції.

Перелік посилань

[1] П. Автор, *Назва книги*. Редактор. Київ, 1990. 234 с.

[2] П. Автор, В. Автор, *Назва статьї*, Назва журнала 20 (5) (1995). 10-15 с.

[3] П. Автор, *Назва доповіді.* В Д. Редактор (ред). Збірник доповідей Національного Симпозіуму з Міжнародною участю «Метрологія та метрологічне забезпечення 2000», (Созополь. 13-17 Сентября 2000), ТУ – София, Болгария 2000, с. 123-127.

References

[1] P. Avtor, *Nazva knyhy*, Redaktor. Kyiv, 1990. 234 s.

[2] P. Avtor, V. Avtor, *Nazva stati*, Nazva zhurnala 20 (5) (1995). 10-15 s.

[3] P. Avtor, *Nazva dopovidi.* V D. Redaktor (red). Zbirnyk dopovidei Natsionalnoho Sympoziumu z Mizhnarodnoiu uchastiu "Metrolohiia ta metrolohichne zabezpechennia 2000", (Sozopol. 13-17 Sentiabria 2000), TU – Sofyia, Bolharyia 2000, s. 123-127.

Реферат

Кулій Ростислав;
Степаненко Олександр
Назва статті

У роботі представлені вимоги щодо оформлення статей для подання у збірник «Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні».

Кулий Ростислав;
Степаненко Александр;
Название статьи

В работе представлены требования по оформлению статей для представления в сборник «Правовое, нормативное и метрологическое обеспечение системы защиты информации в Украине».

Kulii Rostislav;
Stepanenko Olexander
Article title

The paper presents the requirements for registration of articles for submission to the collection «Legal, regulatory and metrological support of information security system in Ukraine».

Відомості про авторів

Прізвище Ім'я По-батькові

Освіта: Повна назва спеціальності (рік).

Науковий ступінь: Кандидат відповідних наук (рік) або Доктор відповідних наук (рік).

Вчене звання: Старший науковий співробітник, доцент, професор (рік).

Місце роботи: кафедра, факультет, університет (лабораторія, відділ, організація).

Область знань:

Наукові інтереси:

Email: