МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ КОРАБЛЕБУДУВАННЯ
імені адмірала Макарова

СУЧАСНІ ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ТРАНСПОРТІ

СПІБТ–2021

МАТЕРІАЛИ

IX Всеукраїнської науково-технічної конференції з міжнародною участю

01–03 грудня 2021 року

Національний університет кораблебудування
імені адмірала Макарова
Навчально-науковий інститут автоматики та електротехніки
просп. Центральний, 3, м. Миколаїв

МИКОЛАЇВ • НУК • 2021

УДК 004
У 45

ОРГАНІЗАТОРИ:

1. Міністерство освіти і науки України
2. Національний університет кораблебудування імені адмірала Макарова
3. ТОВ «БЕЗПЕКАІНФОСЕРВІС»
4. Науково-технічний центр «Квант»

Відповідальна за випуск В. В. Трибулькевич

У–45 **Сучасні** проблеми інформаційної безпеки на транспорті: матеріали IX Всеукраїнської науково-технічної конференції з міжнародною участю. – Миколаїв : НУК, 2021. – 219 с.

У збірнику подано матеріали IX Всеукраїнської НТК "Сучасні проблеми інформаційної безпеки на транспорті".

Розглянуті питання теорії та практики систем інформаційної безпеки транспортних засобів і систем, захисту інформації в каналах зв'язку та глобальних мережах передачі даних, захисту інформації на об'єктах інформаційної діяльності та в інформаційно-телекомунікаційних системах, а також питання підготовки кадрів у галузі знань «Інформаційна безпека».

Збірник може бути корисним для наукових співробітників, викладачів, інженерів та студентів.

УДК 004

СЕКЦІЯ 1. ІНФОРМАЦІЙНА БЕЗПЕКА ТРАНСПОРТНИХ ЗАСОБІВ І СИСТЕМ

УДК 316.485.26:316

ВЗАЄМОЗВ'ЯЗОК ПОЛІТИКИ ТА ІНТЕРНЕТ-ПРОСТОРУ: КОНЦЕПТУАЛЬНІ ЗАСАДИ ЕЛЕКТРОННОЇ ДЕМОКРАТІЇ

Автори: *Ключко М.О., студент; Ніколаєнко В.І., студент, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

Науковий керівник: *Ніколаєнко Н.О., д.п.н., професор кафедри адміністративного та конституційного права, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

Розвиток інформаційних і комунікаційних технологій (ІКТ) на сучасному етапі помітно модернізують індустріальне суспільство.. Як якісно новий період у розвитку суспільства набуває актуальності поняття інформаційного суспільства, що характеризується визначальною роллю і високим рівнем розвитку інформаційних технологій. Для інформаційного суспільства характерно створення ефективної системи забезпечення прав громадян і соціальних інститутів на вільне отримання, розповсюдження і використання інформації як найважливішої умови демократичного розвитку, поліпшення взаємодії населення з органами влади.

Одним із засобів, що визначає розвиток інформаційного простору на сучасному етапі, виступає мережа Інтернет, що являє собою глобальну загальнопланетарну інформаційну систему, засіб об'єднання різноманітних інформаційних комп'ютерних мереж для передачі та обміну інформацією між країнами, регіонами, організаціями та індивідуальними користувачами.

Інтернет багатосторонньо впливає на різні політичні процеси. До переваг використання Інтернету в політичному процесі відносять: низька вартість та оперативність поширення інформації; мультимедійні можливості, тобто поєднання візуальних, звукових, відео- та інших ефектів для впливу на органи відчуття людини; індивідуалізація – мережа задовольняє інформаційні потреби як окремо взятої особистості,

так і груп людей; можливість реалізації глобальних маніпулятивних впливів, використання всіх ресурсів гіпертексту для прокладання необхідних маршрутів маніпулятивних кампаній; інтерактивність – можливість діалогу в процесі обміну інформацією, на відміну від монологу у взаємодії з традиційними ЗМІ; безкарність, можлива анонімність комунікатора, прихований вплив на мережеві спів товариства й особистість в Інтернеті; технічні можливості Інтернету дозволяють не тільки створювати мережі й впливати на споживачів інформації, а й проводити моніторинг мереж, визначаючи можливі мережі й адреси поширювачів тієї чи іншої інформації; задоволення особистісних, комунікативних потреб за рахунок використання телекомунікаційних технологій; відсутність посередників, що спрощує взаємодію між громадянами та владою.

Отже, перспективний потенціал Інтернету на сьогодні – саме в залученні громадян до політичних процесів та реальних можливостях для політичних змін. Крім того, Інтернет дозволяє радикально підвищити ефективність державного механізму в цілому. Перенесення політичними акторами частини своєї комунікаційної діяльності в мережу Інтернет сприяє формуванню принципово нового типу інтерактивної комунікації.

Серед новітніх форм політичної комунікації особливе місце займає електронна демократія (е-демократія). Теоретичні основи концепції е-демократії ведуть свій початок із США та Великої Британії. Саме там вперше було введено до наукового обігу термін «електронна демократія» (e-democracy). В основі концепції е-демократії, перш за все, лежить можливість громадян відкрито виявляти свою політичну активність за допомогою комп'ютерних комунікацій. Е-демократія передбачає застосування новітніх інструментів обміну інформацією, засобів зв'язку держави і громадян.

Е-демократія знаходить вияв у таких формах: організація голосування через світову мережу; надання громадянам можливості обговорення рішень органів влади на форумах, у чатах, блогах; «демократія з відкритим кодом» (open source democracy), що передбачає спільну законотворчість парламенту і громадян; «електронний уряд» (е-

Government), що вимагає від урядових установ в обов'язковому порядку відображати процес своєї діяльності в онлайн-режимі; «електронне-урядування» (e-Governance), «напівпряма е-демократія» (semi-direct e-democracy), що передбачає попереднє обговорення законопроектів у мережі Інтернет до їх ратифікації (або подання у парламент); е-консультації через дискусійні форуми. У США активно використовується така форма е-демократії як комп'ютерне лобіювання, що передбачає використання комп'ютерних мереж як інформаційного ресурсу; прямий інформаційний тиск через комп'ютерні мережі; використання комп'ютерних мереж для приватного спілкування з представниками державної влади або органів місцевого самоуправління.

Отже, серед форм політичної комунікації особливу роль у комунікаційному процесі відіграє е-демократія, теоретичні основи якої продовжують розроблятися і знаходять практичне застосування.

Активне впровадження механізмів е-демократії як засобів впливу на управління та керівництво державою позитивно позначається на політичній участі населення. Використання новітніх технологій громадянами не тільки в особистих цілях, але і в якості суспільно-політичної участі на всіх рівнях публічного управління формує новий рівень активності громадян. Залучення більшої кількості людей до політичного процесу забезпечує реалізацію їхніх інтересів, сприяє відкритості політичної влади, допомагає спілкуванню громадян із владою.

Однак, варто звернути увагу на негативні тенденції впливу Інтернету на формування політично активної особистості. Влада отримала потужний засіб впливу і управління поведінкою людей через швидкий доступ до будь-якої інформації про конкретну особу, організацію чи інститут. Розвиток сучасних технологій може бути використано для тотального контролю з боку держави над своїми громадянами. Крім того, державні органи в ряді країн (Китай, Північна Корея) намагаються контролювати Інтернет-комунікації. Тим самим до наукового дискурсу, поряд із поняттям «медіакратія», введено такі поняття як «медіаімперіалізм», «культурний імперіалізм», «інформаційно-фінансовий імперіалізм».

Департамент економічного і соціального розвитку ООН щорічно оприлюднює огляди готовності країн світу до використання е-урядування. Оцінка здійснюється за двома критеріями:

– *індексом розвитку електронного уряду* (e-Government Development Index (EGDI));

– показниками електронної участі населення (e-Participation).

У свою чергу EGDI включає такі показники: *онлайн сервіси* (Online Service Index) включають електронні інформаційні ресурси органів влади; *розвиток телекомунікаційної інфраструктури* (Telecommunication Infrastructure Index) демонструє кількісні показники (кількість телефонних ліній, загальне число користувачів Інтернет, кількість персональних комп'ютерів, телевізорів і мобільних телефонів на тисячу жителів); *індекс людського капіталу* (Human Capital Index) показує, яка кількість людей має можливість користуватися електронними послугами.

Список літератури:

1. Василевич Ю. В. Інформаційно-комунікаційні технології в політиці: електронна демократія, Україна і світ: теоретичні й практичні аспекти сучасного політичного процесу : колективна монографія, кер. кол. авт. і наук. ред. д. політ. н., проф. Н. О. Ніколаєнко, Херсон : Грінь Д. С., 2016, 520 с., С. 234–268.

2. Грицяк Н. В. Електронна демократія як механізм політичної взаємодії : навч.-метод. рек., К. : НАДУ, 2013, 44 с.

3. Громадська Н. А. Сучасні особливості політичної комунікації та її прояви в інформаційному суспільстві, Наукові праці [Чорноморського державного університету імені Петра Могили комплексу «Києво-Могилянська академія»]. Серія : Політологія, 2014,Т. 248, Вип. 236, С. 53–58.

4. Клімушин П. С. Електронне урядування в інформаційному суспільстві : монографія, Х. : Магістр, 2010, 312 с.

5. Міносян А. С. Електронна демократія в сучасному світі: досягнення та проблеми . – URL: http://www.nbuv.gov.ua/portal/soc_gum/Vdnuet/gum/2011_2/Minosan.pdf

6. What is Good Governance? [Electronic resource] // United Nations Economic and Social Commission for Asia and the Pacific. – URL: http://www.unescap.org/sites/default/files/good-governance.pdf

УДК 316.485.26:316.77

ОСОБЛИВОСТІ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Автор: *Кузьміна А.І., студентка, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

Науковий керівник: *Ніколаєнко Н.О., д.п.н., професор кафедри адміністративного та конституційного права, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

Визначення XXI ст.століттям інформації підкреслює її панування в сучасному світі. Інформація стала продуктивною силою і товаром, засобом захисту і нападу у відстоюванні особистих, суспільних і державних інтересів. З її зростаючою роллю в житті сучасного суспільства проблема інформаційної безпеки вимагає до себе постійної і більшої уваги.

Інформаційна безпека є складним, системним, багаторівневим явищем, на стан і перспективи розвитку якого здійснюють прямий вплив зовнішні і внутрішні чинники, серед яких: 1) політична обстановка у світі; 2) наявність потенційних зовнішніх і внутрішніх загроз; 3) стан і рівень інформаційно-комунікаційного розвитку країни; 4)внутрішньополітична обстановка в державі.

До ключових понять у сфері забезпечення інформаційної безпеки відносять наступні: «інформація», «інформаційна сфера», «безпека», «інформаційна безпека», «безпека інформаційної сфери». Категорія «інформація» є засобом комунікації людей, одним із найважливіших факторів системи суспільних відносин. Поняття інформації неодноразово змінювалось, тому точного й однозначного визначення поняттю немає.

Інформація (лат. informazio – роз'яснення, виклад, поінформованість) – одне з найбільш загальних понять, що позначає певні відомості, сукупність будь-яких даних, знань тощо. Саме поняття «інформація» зазвичай передбачає наявність принаймні трьох об'єктів: джерела інформації, її споживача та середовища, через яке передається інформація.

Інформація – це документовані або публічно оголошені відомості про події та явища, що відбуваються у суспільстві, державі та навко-

лишньому природному середовищі (Закон України «Про інформацію» від 02.10.1992 р.).

З огляду на сприйняття інформаційної сфери безпосередньо як інформації та сфери її обігу, безпека інформаційної сфери – це стан захищеності інформації та сфер її створення, накопичення, зберігання, оброблення, розповсюдження й використання. Інформаційна безпека визначається як стан захищеності життєво важливих інтересів людини, суспільства й держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив: негативні наслідки застосування інформаційних технологій; несанкціоноване поширення, використання, порушення цілісності, конфіденційності та доступності інформації.

Інформаційна безпека стан захищеності особи, суспільства й держави, при якому досягається інформаційний розвиток (технічний, інтелектуальний, соціально-політичний, морально-етичний), за якого сторонні інформаційні впливи не завдають їм суттєвої шкоди. У політичній сфері об'єктами інформаційної безпеки виступають: суспільна свідомість та політична орієнтованість суспільних верств і населення окремих регіонів країни; система вироблення, прийняття і впровадження політичних рішень; права політичних партій, організацій, громадських об'єднань; система інформування населення про політичне, економічне та інше життя країни; система формування громадської думки, до якої входять інституції вивчення та аналізу громадської думки. Відповідно, у духовній сфері – світогляд людини, її життєві цінності та ідеали; соціальні та особистісні орієнтації; культурні та естетичні позиції. Об'єктами інформаційної безпеки у сфері економіки є інформаційно-аналітична система державної статистики; джерела інформації про комерційну діяльність суб'єктів усіх форм власності; інформаційно-аналітичні системи збору та обробки фінансової, податкової, митної, зовнішньоекономічної інформації. У галузі оборони до таких об'єктів відносять інформаційно-аналітичні системи, інформаційні ресурси апарату Міноборони; інформаційні ресурси військово-оборонних підприємств та науково- дослідних установ, які працюють у цій галузі; систе-

ми зв'язку та управління військами та зброєю; морально-психологічний стан Збройних сил України. Основні напрямки забезпечення інформаційної безпеки пов'язані зі станом захищеності людини і громадянина, суспільства, держави. Інформаційна безпека особистості – це стан захищеності особистості, соціальних груп чи об'єднань від негативних впливів деструктивної інформації, що призводить до зміни психічних та психологічних характеристик людини, її поведінки та сприйняття дійсності; здатність держави створити належні умови для гармонійного розвитку й задоволення потреб особистості в інформації.

До інформаційних загроз особистості відносять: втручання в особисте життя, використання об'єктів інтелектуальної власності, деформація системи масового інформування та поширення дезінформації, обмеження доступу до інформації, посилення інформаційно-психологічного впливу на людину тощо. Інформаційна безпека суспільства – це можливість вільно реалізовувати суспільством та окремими його членами свої конституційні права на безперешкодне одержання, обробку, створення й поширення інформації, а також ступінь їх захисту від деструктивного інформаційного впливу. Інформаційна безпека держави – це захист основних сфер життєдіяльності держави від небезпечних (дестабілізуючих, деструктивних, що уражають державні інтереси і т. ін.) інформаційних впливів; конкретні дії щодо забезпечення безпечних умов існування інформаційних процесів та їх безпечного розвитку в майбутньому; забезпечення безпечних умов існування інформаційних технологій, які включають питання захисту інформації, інформаційної інфраструктури держави, інформаційного ринку та створення безпечних умов існування та розвитку інформаційних процесів. Комплекс питань інформаційної безпеки держави включає такі сфери державної діяльності, як: захист та обмеження обігу інформації; захист інформаційної інфраструктури держави; безпека розвитку інформаційної сфери держави; захист національного інформаційного ринку; попередження інформаційного тероризму та інформаційної війни. Інформаційна безпека держави відіграє важливу роль у забезпеченні інтересів будь-якої держави та позначає стійкість основних сфер її життєдіяльності відносно небезпечних інформаційних впливів, причому як до впровадження, так і до викрадення інформації. Визначається здатністю нейтралізувати такі впливи.

Основні напрямки роботи в сфері інформаційної безпеки держави: формування законодавчої і нормативно-правової бази забезпечення інформаційної безпеки, включаючи визначення правового статусу суб'єктів системи інформаційної безпеки, захист та обмеження обігу інформації, розробка механізмів реалізації прав громадян на інформацію, дослідження форм і способів цивілізованого впливу держави на формування суспільної свідомості, захист інформаційної інфраструктури держави, захист моральних цінностей, безпека розвитку інформаційної сфери держави, захист національного інформаційного ринку, попередження несанкціонованого доступу до інформації, інформаційного тероризму та інформаційної війни.

Завдання забезпечення інформаційної безпеки держави: виявлення, оцінка та прогнозування поведінки джерел загроз інформаційній безпеці, що здійснюється шляхом оперативного моніторингу інформаційної обстановки; мінімізація шкоди через неповноту, несвоєчасність або недостовірність інформації чи негативного інформаційного впливу через наслідки функціонування інформаційних технологій, а також несанкціоноване поширення інформації; створення та експлуатація систем забезпечення інформаційної безпеки; розробка, координація та запровадження єдиної державної політики у галузі міжнародних інформаційних відносин, зокрема у напрямку формування іміджу держави.

Інформаційна безпека є складним, системним, багаторівневим явищем, на стан і перспективи розвитку якого здійснюють прямий вплив зовнішні і внутрішні чинники, серед яких: політична обстановка у світі; наявність потенційних зовнішніх і внутрішніх загроз; стан і рівень інформаційно-комунікаційного розвитку країни; внутрішньополітична обстановка в державі. Інформаційна безпека держави відіграє важливу роль у забезпеченні інтересів будь-якої держави та позначає стійкість основних сфер її життєдіяльності відносно небезпечних інформаційних впливів, причому як до впровадження, так і до викрадення інформації.

Список літератури:

1. Богуш В. М. Інформаційна безпека держави / В. М. Богуш, О. К. Юдін. – К. : «МК-Прес», 2005. – 432с., іл.

2. Жарков Я. М. Інформаційна безпека особистості, суспільства, держави : підручник / Я. М. Жарков, М.Т. Дзюба, І. В. Замаруєва [та ін.]. – К. : Видавничо-поліграфічний центр «Київський університет», 2008.– 274 с.

3. Інформаційна безпека суспільства і держави. Стратегічні цілі і задачі інформаційної боротьби.[Електронний ресурс]. – Режим доступу: http://www.ngo.dn.ua/doc/concept.doc. – Назва з екрану.

4. Політологія : навчальний енциклопедичний словник-довідник для студентів ВНЗ I–IV рівні акредитації/ за наук. ред. д-ра політ. н. Н. М. Хоми [В. М. Денисенко, О. М. Сорба, Л. Я. Угрин та ін.]. – Львів : Новий Світ-2000, 2014. – 779 с.

5. Степко О. М. Аналіз головних складових інформаційної безпеки держави [Електронний ресурс] /Олександр Михайлович Степко // Науковий вісник Інституту міжнародних відносин НАУ. Серія:економіка, право, політологія, туризм. – 2011. – Т. 1, № 3. – Режим доступу:http://jrnl.nau.edu.ua/index.php/IMV/article/view/3214/3172. – Назва з екрану.

6. Ярочкин В. И. Информационная безопасность : учебник для студентов вузов / В. И. Ярочкин. – М. :Академический Проект ; Фонд «Мир», 2003. – 640 с.

УДК 316.485.26:316

ІНФОРМАЦІЙНА БЕЗПЕКА В ПУБЛІЧНОМУ УПРАВЛІННІ

Автор: *Мороз Л.В., студентка, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

Науковий керівник: *Ніколаєнко Н.О., д.п.н., професор кафедри адміністративного та конституційного права, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

Інформаційна безпека – стан захищеності життєво важливих інтересів людини і громадянина, суспільства і держави, при якому запобігається завдання шкоди через неповноту, несвоєчасність і недостовірність поширюваної інформації, порушення цілісності та доступності інформації, несанкціонований обіг інформації з обмеженим доступом, а також через негативний інформаційно-психологічний вплив та уми-

сне спричинення негативних наслідків застосування інформаційних технологій [1].

Сучасна Україна повинна скласти таку систему забезпечення інформаційної безпеки, яка дозволить гарантовано зберегти національні інтереси за будь – яких умов. На теперішній час проблематика інформаційної безпеки держави досліджується в працях українських вчених, таких як: І.В. Арістової, В.К. Гіжевського, І.П. Голосніченко, Ю.В. Іщенко, Р.А. Калюжного , В.А. Ліпкана та інші.

Але їх дослідження стосувалися тільки вивченню проблеми національної безпеки в інформаційній сфері, саме тому на цей час ще залишається недостатньо вивченими концептуальні положення системи забезпечення інформаційної безпеки держави, і це є очевидною проблемою в країні. Потреба у захисті стосується і інформації , що міститься не лише у інформаційних системах і передається мережею, а й тією, що знаходиться «поза кадром», тобто існує за закритими дверима (особисте листування, данні відділу кадрів, матеріали обговорення питань у залах сесійних засідань, в кабінетах різних комітетів, міністерств і комісій). Більшість державних органів додержуються основних базових принципів гарантування інформаційної безпеки, а саме – використання інформації у відповідності з законодавством і саме з тією метою, з якою вона надається; зведення обсягу інформації до необхідного мінімуму; повага до прав громадян, суспільства або організацій, яких ця інформація стосується безпосередньо; своєчасне оновлення, забезпечення актуальності і достовірності інформації; збереження необхідної інформації до тих пір поки вона є необхідною; постійна підтримка безпеки інформаційного середовища; надання інформації іншим органам та організаціям лише після надходження відповідних запитів і здійснення відповідних захисних задів.

Механізм публічного управління інформаційною безпекою особистості у сфері національної безпеки являє собою спільну діяльність органів державної влади, місцевого самоврядування, які разом із залученими громадськими організаціями, окремими особами, притаманними їм нормативно регламентованими методами та інструментами забезпечують відповідне реальності сприйняття людиною соціально

значимої інформації з метою захисту суверенітету, територіальної цілісності держави, національних цінностей, конституційного ладу, дотримання законності, правопорядку, створення умов для всебічного і гармонійного розвитку людини, подолання звичок, які є шкідливими для людини [2].

В сучасному світі людство зазнає бурхливий розвиток інформатизації, автоматизації та комп'ютеризації всіх сфер життя. Це все створює нові можливості для розвитку національної економіки, освіти, культури та науки. Проте є і негативні аспекти : поширення інформаційних технологій відкриває шляхи до злочинної поведінки та антисоціальної злочинності. Комп'ютерні системи надають нові, найдосконаліші , можливості для невідомих раніше правопорушень, для скоєння традиційних злочинів, але нетрадиційними методами.

Кожна держава, захищаючи свої інформаційні інтереси, має дбати про свою інформаційну безпеку. Зміцнення української державності також цього вимагає, виходячи з пріоритетності національних інтересів та загроз національної безпеці країни. Спираючись на правову точку зору, вона ґрунтується на основах правової демократичної держави і запроваджується шляхом розробки та реалізації відповідних національних доктрин, стратегій, різних концепцій та програм згідно із чинним законодавством. Наразі в Україні є об'єктивна потреба у державно – правовому регулюванні науково – технологічної та інформаційної діяльності, яка б відповідала реаліям сучасного світу та ступеню розвитку інформаційних технологій, нормами міжнародного права, але заразом ефективно захищала б приватні українські національні інтереси. Всі відносини, які тим чи іншим шляхом, пов'язані із забезпеченням інформаційної безпеки країни, як найважливіші на теперішній час для суспільства та держави вимагають прискореного законодавчого регулювання[2].

Таким чином, інформаційну безпеку слід розуміти як сукупність засобів забезпечення інформаційного суверенітету України, захист інформаційної сфери від загроз – внутрішніх та зовнішніх, яка має включати ефективну протидію сукупності інформаційних загроз[4].

Головна інформаційна загроза національній безпеці будь – якої країни і України зокрема – це загроза впливу іншої сторони на інформаційну інфраструктуру країни, інформаційні ресурси, на суспільство,

свідомість, підсвідомість особистості, і має головну мету – нав'язати державі бажану, для іншої сторони , систему поглядів, інтересів, цінностей і ухвал у життєво важливих сферах державної та суспільної діяльності, верховодити їхньою поведінкою і всебічним розвитком у бажаному для іншої сторони напрямку[5].

Саме це є загрозою суверенітету України в життєво важливих сферах суспільної й державної діяльності, що реалізується на інформаційному рівні.

Україна, як частина світового інформаційного простору, має виробити сукупність заходів для власного сталого інформаційного розвитку в умовах жорсткої конкуренції з урахуванням всіх аспектів інформаційної безпеки. Саме для цього необхідно :

– розуміння інформаційних атак та протистояння ним;

– створення програмного забезпечення протистояння інформаційним атакам;

– аналіз показників інформаційних загроз з метою вдосконалення механізмів прийняття рішень в системах державного управління;

– забезпечення максимального захисту від зовнішніх впливів;

– аналіз технічного стану всіх засобів комунікації;

– поєднання діяльності органів державної влади та засобів масової інформації у сфері політичного інформування суспільства для нейтралізації негативного психологічного впливу в умовах конфліктів та криз.

Всі види інформаційних технологій, їхнього виробництва та засоби забезпечення цих технологій становлять спеціальну сферу діяльності, розвиток якої визначається державною інформаційною політикою та Національною програмою інформатизації. Питання визначення завдань Національної програми інформатизації, пріоритетних напрямів розвитку інформатизації, обсягів, джерел і порядок їх фінансування, покладено на Кабінет Міністрів України і затверджуються щорічно Верховною Радою України.

В інформаційній сфері, національну безпеку України, слід розглядати як єдину цілісність чотирьох складових – публічної (суспіль-

ної), персональної, корпоративної (комерційної) і державної безпеки. Саме тому, при окресленні характеру ризиків слід брати до уваги наступні елементи:

– основні елементи політичної безпеки, її принципів, стандартів та правил, погоджених із чинним законодавством й принципами забезпечення безперервності системи інформаційної безпеки особистості, суспільства, корпоративних структур та держави;

– визначення об'єктів та цілей;

– визначення прийнятих з погляду забезпечення інтересів усіх суб'єктів структур встановлення контролю над об'єктами безпеки, а також оцінки ризиків та управління ризиками;

– визначення статусно – функціональних ролей, очікування та міри відповідальності задіяних суб'єктів включно зі звітністю про події, які несуть потенційні загрози[6].

Список літератури:

1. Про Доктрину інформаційної безпеки України: Указ Президента України від 25.02.2017 р. №47/2017. URL: https://zakon.rada.gov.ya/laws/show47/2017#Text

2. Бондар І. Інформаційна безпека як основа національної безпеки, Механізм регулювання економіки,Суми, 2014.

3. Публічне управління: термінол. слов., уклад.: В.С. Куйбіда та ін.; за заг. ред. В.С.Куйбіди, М.М.Білинської, О.М.Петроє. Київ: НАДУ, 2018, 224 с.

4. Шатіло В.А. Теоретичні проблеми конституційного механізму державної влади: співвідношення організаційних структур та функцій (вітчизняний і світовий досвід): монографія. Київ:Юридична думка, 2017, 364 с.

5. Малімон В.І., Дівнич В.М. співвідношення механізмів державного управління й механізмів державної підтримки. Право і суспільство. 2015. №5.2. с.127-133. URL: https:// nbuv.gov.ua/UJRN/Pis_2015

6. Механізми реформування і реалізації державної політики протидії злочинності у сфері національної безпеки України: наук. – прак. посіб., за ред. В,П, Горбоуліна. Київ: Євроатлантикінформ, 2006, 268 с.

УДК 316.485.26:316.77

КОМУНІКАЦІЙНІ ТЕХНОЛОГІЇ В ІНФОРМАЦІЙНОМУ ПРОСТОРІ

Автори: *Ніколаєнко Н.О., д.п.н., професор кафедри адміністративного та конституційного права; Ключко О.О., студент, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

В інформаційному просторі суспільства використовуються різні комунікаційні технології, призначення яких полягає в тому, щоб сформувати певну громадську думку, відповідним чином сконструювати сприйняття політичних реалій і забезпечити підтримку тих чи інших політичних рішень, тобто отримати конкретний результат. Комунікаційні технології у сучасному світі здатні найбільш ефективно виконувати завдання створення та підтримки простору демократичного діалогу між політичною сферою, владою та громадянами. Вони ґрунтуються на знаннях про людину, її буття і реалізуються як системні інтелектуальні комплекси, спрямовані на маніпулювання свідомістю.

У процесі демократизації політичної системи важливу роль відіграють саме комунікаційні технології, призначення яких полягає у налагодженні прозорих суспільних комунікацій як між органами державної влади та місцевого самоврядування, так і інститутами громадянського суспільства.

Політико-комунікаційні технології, відіграючи провідну роль у системі управління суспільством і процесами, що відбуваються в ньому, відрізняються системною природою, визначають суспільну організацію, характеризуються структурно-функціональним змістом.

Типи комунікаційних технологій (О. Соловйов):

1) ринкові (або маркетингові) – паблік рилейшнз, політична реклама, інформаційний лобізм тощо;

2) неринкові (або немаркетингові) – політична пропаганда, політична агітація.

Відповідно до іншої типології існують такі технології політичної комунікації (Д. Наріжний):

- PR технології;
- виборчі технології;
- технології політичної реклами;
- технології політичного впливу і маніпулювання;
- технології формування політичного іміджу;
- технології міжнародних політичних комунікацій.

Із розвиток процесів модернізації та індустріалізації суспільства до наведених переліків політико-комунікаційних технологій додалися перфоманс і резонансні технології. Зміст останніх полягає в тому, що вони є прикладом т. зв. «м'якої могутності», що використовується у демократичних суспільствах та враховує когнітивні, комунікативні та власне резонансні схеми, за якими живе аудиторія. Резонансна комунікація будується на активізації тих уявлень отримувача інформації, які він уже має.

Політичний перфоманс – це спеціальна, як правило, символічна, зазвичай ритуальна діяльність, що здійснюється індивідом або групою осіб із метою справити враження на іншого індивіда, групу або масу людей і привернути увагу до своєї діяльності та функціонування. Він реалізується у спланованих та організованих політичним суб'єктом діях для нарощення власного пабліцитного капіталу. Перфоманс передбачає спонтанності; в ньому є організація та чітка ієрархія; він переслідує певні цілі і не розрахований на випадкових глядачів, організатори вибирають місце і час із метою найбільшого впливу на аудиторію. Використання політичного перфомансу дає певну гарантію привернення уваги аудиторії до політичних проблем.

Призначення політичних технологій у політичній комунікації полягає в тому, що вони є механізмами управління інформаційними процесами в політиці та носіями політичної інформації.

Самостійною складовою системи політичних комунікацій є політична пропаганда.

Пропаганда – це давній інструмент впливу на громадську думку. Історично це явище пов'язане з періодами напруги соціальних потрясінь та політичних конфліктів. Поступово пропаганда ставала основним інструментом контролю громадської думки та ефективною «м'якою» зброєю в боротьбі з противником. Із плином часу смисловий зміст пропаганди змінився, вона стала асоціюватися з неправдою та оманою.

Термін «пропаганда» сягає корінням назви католицької організації Sacra Congregatio de Propaganda Fide (Священна конгрегація розповсюдження віри), що була створена в 1622 році для поширення віровчень Римо-католицької церкви на Новий Світ та протистояння руху протестантської Реформації в Європі.

Політична пропаганда є невід'ємною умовою здобуття, утримання та реалізації влади. Вона популяризує та прищеплює масовій свідомості визначені політичні ідеї та ідеали.

Типи пропаганди:

1) відповідно до джерела повідомлення:

– *«біла» пропаганда* загалом походить із відкритого доступного джерела та характеризується м'якими методами переконання, такими як стандартні техніки відносин із населенням та однобічним поданням аргументів;

– *«сіра» пропаганда* направлена на те, щоб змусити повірити в неправдиву інформацію;

– *«чорна» пропаганда* – це сфабрикована неправдива інформація (або просто відверта брехня), поширення якої має на меті спровокувати політичний, соціальний, міжетнічний або міждержавний конфлікт.

2) відповідно до природи повідомлення:

– *позитивна (конструктивна) пропаганда* прагне донести до споживача ті або інші переконання в доступній формі, тим самим виконує виховну та інформаційну функції в суспільстві. Її мета полягає в тому, щоб сприяти соціальній гармонії, злагоді, вихованню людей згідно із загальноприйнятими цінностями;

– *негативна (деструктивна) пропаганда* використовується для маніпулювання масами в інтересах невеликої групи осіб. Її ціль – розпалювання соціальної ворожнечі, нагнітання соціальних конфліктів, загострення суперечностей у суспільстві тощо.

3) за суб'єктом впливу: державна, партійна і громадська пропаганда;

4) за метою впливу:

– *пропаганда створення* (покликана переконати в необхідності побудови чогось нового (інституту, суспільства), пропонує приєднуватися до цього процесу;

– *пропаганда руйнування* (переконує у наявності ворога, який щось задумує проти нас;

– *пропаганда роз'єднання* (розпалює ворожнечу);

– *пропаганда залякування* (запевняє вірогідного/можливого противника у власній економічній силі);

– *пропаганда відчаю* (наголошує на безнадійному становищі можливого противника, примушує його здатися);

– *пропаганда героїзму* (закликає до згуртування навколо певних цінностей, допомагає легше пережити складнощі, ілюструє приклади, до яких необхідно прагнути);

– *пропаганда просвітництва* (повідомляє населення про дії керівництва різного рівня, рекламує спосіб життя).

Якщо говорити про структуру пропаганди, то вона є чітко визначеною та важливою для досягнення поставлених цілей. Пропаганда передбачає наявність ідеї, цільової аудиторії і засобів, щоб донести ідею до потрібної аудиторії.

Основні структурні компонентами пропаганди: 1) адресант; 2) інформація (меседж); 3) джерело інформації; 4) адресат(и).

Політична пропаганда вдається до маніпулювання.

Основні типи маніпуляції свідомістю: переконання, психологічне зараження, наслідування та навіювання (сугестія).

Доповнює пропаганду агітація, методи якої спрямовані на досягнення миттєвого або короткочасного ефекту. *Політична агітація* – це система заходів, які мають за мету сформувати певну політичну позицію і певну політичну поведінку, яка і виражається потім у підтримці чи непідтримці суб'єктів політичного чи виборчого процесів.

Основними прийомами агітації та пропаганди є дезінформація, фальсифікація та маніпулювання свідомістю реципієнтів. Таким чином, комунікаційні технології агітаційно-пропагандистського типу в цілому спрямовані на контроль за розумом і поведінкою людей.

Список літератури:

1. Абудецька Н. Маркетингові засоби комунікації в політиці, Політичний менеджмент, 2011, № 4, С. 105–111.

2. Гойман О. О. Маніпулювання масовою свідомістю в умовах сучасної гібридної війни, Грані, 2015, № 1, С. 50–56.

3. Денисюк С. Г. Технологічні виміри політичної комунікації,Вінниця : ВНТУ, 2010, 276 с.

4. Кравчук М. А. Політична пропаганда як засіб становлення і трансформації політичних режимів : автореф. дис... канд. політ. наук: 23.00.02 ; Львів. нац. ун-т ім. І. Франка. Л., 2006.,19 с.

5. Наріжний Д. Ю. Аналіз політичних технологій та особливостей їх застосування в транзитивному суспільстві : автореф. дис... канд. політ. наук: 23.00.02, Дніпропетр. нац. ун-т. – Дніпропетровськ, 2004, 22 с.

6. Павлов Д. Політична пропаганда: до визначення поняття, Гілея: науковий вісник, 2013, Вип. 79, С. 328–331.

7. Соловьев А. И. Политическая коммуникация: к проблеме теоретической идентификации, Политические исследования, 2002, № 3,С. 5–18.

8. Хома Н. М. Політичний перфоманс як постмодерна форма соціального протесту, Вісник НТУУ «КПІ». Політологія. Соціологія. Право : збірник наукових праць. – 2014. – № 1 (21),С. 18–22.

УДК 316.485.26:316.77

ІНФОРМАЦІЙНА БЕЗПЕКА УКРАЇНИ В УМОВАХ ТРАНСФОРМАЦІЇ СУСПІЛЬСТВА ТА ЗОВНІШНЬОЇ АГРЕСІЇ

Автор: *Нофенко А.С., аспірант кафедри психології та соціальних наук, Миколаївського національного університету ім. В.О. Сухомлинського, м. Миколаїв, Україна*

Науковий керівник: *Ніколаєнко Н.О., д.п.н., професор кафедри адміністративного та конституційного права, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

Еволюція суспільних відносин у розвинутих країнах, що призвела ці країни до створення розвиненої економіки та високого рівня споживання, призвела і до значного зростання потоку різноманітної інформації, що неминуче зажадало створення та постійного розвитку різ-

них інформаційних технологій. А це, у свою чергу, призвело до створення новітньої формації – інформаційного суспільства.

Таким чином, можна говорити про те, що інформаційне суспільство це фаза сучасної цивілізації. Її появі ми зобов'язані інформаційній революції, інструментом якої стала загальна комп'ютеризація практично всього населення розвинених країн, та можливості використання комп'ютерної техніки на виробництві та в побуті, що дає практично кожній людині можливість отримання будь-якої необхідної інформації. На цьому ґрунті відбулися серйозні зміни в системі суспільних відносин, що забезпечили реальну можливість самореалізації особистості.

У сучасному світі інформаційне суспільство розвивається з дуже великою швидкістю і продовжує набирати обертів. При переході від індустріального суспільства до інформаційного, цінність такого ресурсу, як інформація стала не порівнянна з цінністю матеріальних чи енергетичних ресурсів.

В даний час завершується перехід від індустріального суспільства до інформаційного. Праця людини робиться меншою мірою фізичною, більшою – інтелектуальною. Сучасна людина має вільно орієнтуватися в постійно зростаючому потоці інформації, вміти працювати з нею.

Найпотужнішим підсилювачем інтелектуальних здібностей за всю історію розвитку цивілізації є комп'ютер та глобальні мережі. При цьому інформатизація освіти є необхідною умовою розвитку такого суспільства, яке в останні роки неможливо уявити без використання ресурсів мережі Інтернет. Світ освіти наповнюється мережевими сервісами та цифровими ресурсами, кількість яких з кожним роком стрімко збільшується.

В умовах активної модернізації системи освіти змінюється і педагогічна діяльність. Освіта як найважливіша частина життя людини має забезпечувати йому можливість орієнтуватися в потоці інформації, дозволити комфортно почуватися в інформаційному суспільстві, легко адаптуватися до нових тенденцій.

Рівень інформаційної безпеки, як в державних структурах, так і в сфері господарської діяльності, багато в чому визначається якістю підготовки працюючих там спеціалістів, отримавши освіту за різними напрямками об'єднаним областю знань «Інформаційна безпека». Ефективність їх потуг, спрямованих на захист інтересів суб'єктів інфор-

маційних відносин залежить, перш за все, від вміння виявляти та оцінювати загрози, визначати стан захищеності інформації, обґрунтовано обирати засоби її захисту від сукупності реальних загроз, розробляти та впроваджувати системи захисту на базі вимог чинного законодавства України.

Питання інформаційної безпеки в сучасній Україні стоїть так само гостро, як і питання динамічного економічного розвитку та інтеграції у світове співтовариство. Інформація, поряд з фінансовими та природними ресурсами, є найважливішим фактором конкурентоспроможності країни на міжнародній арені. Донедавна проблемам інформаційної безпеки всередині країни та у зовнішньому просторі приділялося вкрай мало уваги.

У зв'язку з цим останніми роками органами законодавчої та виконавчої влади України було прийнято закони та підзаконні акти з питань захисту державної таємниці, забезпечення збереження інформаційних ресурсів держави, їх раціонального використання, регламентації міжнародного інформаційного обміну.

Окремого розгляду потребують норми Закону України «Про інформацію», який є базовим в інформаційному праві, який заклав правові основи захисту інформації з обмеженим доступом. Тут основна увага приділяється таким питанням як: характеристика структури інформаційних відносин та принципи їх правового регулювання; види інформаційних ресурсів та право власності на них; види режиму доступу до інформації та її класифікація згідно з режимом доступу; підстави виникнення відповідальності за порушення законодавства і види такої відповідальності. Оскільки наявність кримінальної відповідальності за окремі порушення є найбільш ефективною мірою захисту законних інтересів власників та користувачів інформаційних ресурсів, треба глибинно вивчати ті види злочинів, передбачених кримінальним кодексом України, предметом яких є інформація або інфраструктура, яка її підтримує [1].

Даючи в цілому позитивну оцінку Закону України «Про інформацію» та характеризуючи його роль в питаннях правового регулювання інформаційних відносин, треба підкреслити, що цей законодавчий акт

не в повній мірі відповідає сучасному рівню розвитку відносин в сфері інформаційної діяльності. Зокрема, регулювання відносин в таких сферах, як інформація про особистість, інформація для службового користування потребує подальшого розвитку на основі розробки та прийняття відповідних законодавчих актів [2]. Невизначеними до теперішнього часу є положення чинного законодавства по відношенню до секретної інформації, яка не складає державну таємницю Накопичений досвід свідчить, що якщо «не ухилятися» від подібних запитань, а ставити їх перед майбутніми фахівцями, то це підвищує їх інтерес до правової проблематики забезпечення інформаційної безпеки та сприяє більш глибокому засвоєнню матеріалу.

Для України з її традиційно високим освітнім рівнем і поки не витраченим інтелектуальним потенціалом є реальний шанс, спираючись на не перерваний інформаційний потік, зробити «ривок» і домогтися відродження втрачених позицій у реальному секторі економіки, використовуючи успіхи освіти та науки як конкурентну перевагу. В умовах «вибухової» еволюції це дає можливість, за необхідними для країни позиціями не лише наздогнати, а й локально перегнати, не наздоганяючи, розвинені країни в повному обсязі.

Однак на цьому тлі багаторазово зростають загрози інформаційної безпеки України. Позиційна, уповільнена інформаційна війна у цій сфері зі своєї традиційної форми плавно починає переходити у відкриту інформаційну війну та загрозу національній безпеці в інформаційній сфері.

У цих умовах, для протидії супротивнику, необхідно точно визначитися з характером загроз. Умовно, основні загрози інформаційній безпеці Україні можна розділити на два типи: зовнішні та внутрішні. До зовнішніх джерел загроз належать: по-перше, відкрита не дружня політика Російської Федерації, спрямована прямо проти економічних інтересів України і, відповідно, із завданням витіснення України із зовнішнього та внутрішнього ринків, особливо у сфері інформації. А це неминуче наводить до загострення конкуренції у сфері виробництва інформаційних ресурсів та технологій. По-друге, таємна, а іноді й явна підтримка діяльності міжнародних терористичних організацій, які є серйозною загрозою для нормального функціонування інформаційних та телекомунікаційних систем, що може призвести до серйозних проблем для ще слабкої економіки України, що відроджується.

До внутрішніх джерел загроз інформаційної безпеки України відносяться: по-перше, суттєво зросла загроза застосування інформаційної зброї проти інформаційної інфраструктури України. Причому, вже не ховаючись, деякі державні діячі, особливо російські, прямо говорять про необхідність застосування такої зброї проти України, ставлячи її в один ряд з міжнародними терористичними організаціями. Розробка країною-агресором стратегій ведення інформаційних воєн, що передбачають створення засобів небезпечного впливу на інформаційні сфери нашої України, порушення нормального функціонування інформаційних та телекомунікаційних систем, збереження інформаційних ресурсів, отримання несанкціонованого доступу до них є одним із реальних джерел зовнішніх загроз національної безпеки нашої держави, не зважати на які, не можуть собі дозволити розсудливі політики.

Питання інформаційної безпеки є ключовими для забезпечення порядку та рівноправності в інформаційному суспільстві. Саме інформаційне суспільство необхідне розглядати як сукупність інформаційних ресурсів, систему формування, поширення та використання інформації, інформаційної інфраструктури.

Ще одна складова національних інтересів України в інформаційній сфері полягає у захисті інформаційних ресурсів від несанкціонованого доступу, забезпечення безпеки інформаційних та телекомунікаційних систем, як уже розгорнутих, і створюваних біля України.

З цією метою необхідно: підвищити безпеку інформаційних систем, включаючи мережі зв'язку, насамперед безпеку первинних мереж зв'язку та інформаційних систем органів державної влади, органів державної влади суб'єктів України, фінансово-кредитної та банківської сфер, сфери господарської діяльності; систем та засобів інформатизації озброєння та військової техніки, систем управління військами та зброєю, екологічно небезпечними та економічно важливими виробництвами; інтенсифікувати розвиток вітчизняного виробництва апаратних та програмних засобів захисту інформації та методів контролю за їх ефективністю; забезпечити захист відомостей, що становлять державну таємницю; розширювати міжнародне співробітництво України в галузі розвитку та безпечного використання інформаційних ресурсів,

протидії загрозі розв'язання протиборства в інформаційній сфері.

Важливим напрямом розвитку інформаційної безпеки має бути соціально-психологічний аспект. Стратегія забезпечення інформаційно-психологічного аспекту безпеки України являє собою довгострокову програму дій у внутрішньому та зовнішньому інформаційному середовищі, узгоджену за цілями, завданнями, умовами, місцем, часом, засобам та ресурсам.

В основу даної концепції має лягти принцип інформації про стратегічний ресурс, а концепція виходити з наступних постулатів: свобода слова, незалежність ЗМІ та свобода друку основа громадянського суспільства; ЗМІ мають працювати на благо свого суспільства та держави; владі слід, доступною мірою, за допомогою інформаційних технологій, керувати ЗМІ у своїй країні, інакше це робитимуть інші держави.

Крім того, важливим аспектом інформаційно-психологічної безпеки є захист від прихованого інформаційного впливу. Фахівці виділяють тут два основні методи: введення інформації в неусвідомлювані зони пам'яті, використовуючи навіювання, роз'яснення, навчання у дистанційному стані тощо; забезпечення прямого доступу на згадку шляхом або зміни стану свідомості, або навіть його відключення.

На закінчення хотілося б відзначити, що затребуваність спеціалістів в області захисту інформації визначається рівнем їх підготовки, що дозволяє вирішувати практичні завдання із попередження або нейтралізації існуючих загроз інформаційній безпеці. Достатній рівень підготовки таких спеціалістів може бути досягнутим тільки із врахуванням необхідності засвоєння ними базових знань в області правового регулювання різноманітної діяльності, кінцевою ціллю якої є захист інтересів законних учасників інформаційних процесів. Це є гарантією не тільки законності такої діяльності, але й, що не менш важливо, її ефективності.

Список літератури:

1. Голубев В. І., Гавловський В. Д., Цимбалюк В. С. Інформаційна безпека: проблеми боротьби зі злочинами у сфері використання комп'ютерних технологій.: монографія, Запоріжжя: Просвіта, 2001, 252 с.

2. Ботвінкін О. В., Ворожко В. П. Інформація з обмеженим доступом, що не є державною таємницею, в законодавстві України. Аналітичний огляд, Київ.: НА СБ України, 2006, 96 с.

СЕКЦІЯ 2. ЗАХИСТ ІНФОРМАЦІЇ НА ОБ'ЄКТАХ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ ТА В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ

УДК 004.056

МЕТОДИКА ЕФЕКТИВНОЇ КОМПОНОВКИ СПЕЦІАЛІЗОВАНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ ЗАХИСТУ КОМП'ЮТЕРНИХ МЕРЕЖ

Автори: *Гратій А.О., магістрант; Турти М.В., к.т.н., доцент, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

Стрімкий розвиток інформаційних технологій, створення відкритого кіберпростору розширює можливості професійної діяльності і суттєво спрощує вирішення побутових проблем сучасної людини. Однак, цифровізація, окрім наочних переваг, має і негативні наслідки, серед яких кіберзлочинність посідає перше місце і завдає шкоди не тільки конкретним особам та організаціям, а й державі в цілому. Протидія кіберзлочинам є складною задачею, яка вирішується в сучасному кіберпросторі за допомогою інтелектуальних систем і нейронних мереж за сценарієм «бот проти бота».

Спеціалізоване програмне забезпечення (ПЗ) для захисту комп'ютерних мереж (КМ) допомагає проводити їх моніторинг, аналізувати в реальному часі отримані результати і автоматично активувати відповідні запобіжні засоби. Відповідно підвищується значимість спеціалізованого ПЗ (СПЗ) в системі захисту інформації (СЗІ). Розробці спеціалізованого ПЗ (СПЗ), вдосконаленню методів його ефективного використання присвячені роботи багатьох вітчизняних та зарубіжних науковців науковців [1-8], в тому числі науковців Національного університету кораблебудування [5, 7, 8].

На даний час існує дуже багато СПЗ для захисту КМ, але методика їх оптимальної компоновки, яка враховувала б особливості СПЗ, їх відповідність вимогам користувача і взаємну узгодженість, а також

особливості програмно-апаратного середовища функціонування, на даний час відсутня.

Метою даної роботи є розробка методики ефективної компоновки спеціалізованого програмного забезпечення для захисту комп'ютерних мереж як складової системи підтримки прийняття рішень (СППР) при формуванні комплексу засобів захисту комп'ютерних мереж.

Для досягнення поставленої мети необхідно вирішити наступні задачі:

– провести аналіз нормативно-правової бази побудови захищених КМ і визначити основні вимоги до спектру функцій комплексу засобів захисту (КЗЗ);

– провести аналіз літературних джерел вільного доступу і визначити доцільні для застосування у даній роботі критерії вибору СПЗ для захисту КМ і методи прийняття рішень;

– розробити методику ефективної компоновки СПЗ для захисту КМ на основі визначених критеріїв і методів прийняття рішень.

В результаті аналізу нормативно-правової бази побудови захищених КМ і відкритих літературних джерел [6] визначимо спектр функцій, які повинен виконувати КЗЗ:

– управління подіями інформаційної безпеки;

– статичний та динамічний аналіз файлів (sandbox, «пісочниця» і аналіз контексту файлів);

– захист веб-трафіку;

– фільтрація мережевого трафіку;

– захист мережевого периметру;

– виявлення кіберзагроз;

– реагування на кіберзагрози;

– антивірусний захист;

– запобігання внесенню несанкціонованих змін в серверні систем;

– створення груп користувачів і надання їм прав доступу до мережевих інформаційних ресурсів і пристроїв;

– аудит дій користувачів;

– контроль змін інформаційних ресурсів (файлів та каталогів);

– контроль використання мережевих пристроїв;

– інвентаризація компонентів IT-інфраструктури;

– оцінка стану технічного захисту інформації в інформаційно-телекомунікаційних системах.

В режимі реального часу КЗЗ може забезпечувати:

– обробку артефактів (виявлення артефактів; моніторинг артефактів; аналіз і реагування на артефакти; створення динамічної бібліотеки артефактів;

– обробку вразливостей (виявлення вразливостей; аналіз і реагування на виявлені вразливості; апаратно-програмне забезпечення виявлення і реагування на виявлені вразливості; інформаційна підтримка і координація реагування);

– обробку інцидентів (виявлення інцидентів; аналіз і реагування на інциденти; апаратно-програмне забезпечення виявлення і реагування на інциденти; інформаційна підтримка і координація реагування на інциденти; служби виявлення вторгнень; ведення журналів інцидентів);

– профілактичні сервіси (моніторинг процесів обробки інформації на об’єкті інформаційної діяльності для певних інформаційних технологій, певних інформаційних ресурсів і мережевих пристроїв, інформації з певним рівнем секретності; аналіз і оцінка поточного стану систем безпеки; конфігурація, реконфігурація і підтримка систем безпеки; служби запобіганню вторгненням; поширення інформації, пов'язаної з безпекою; підвищення кваліфікації персоналу);

– управління якістю систем безпеки (аналіз ризиків; оцінка програмних продуктів і апаратного забезпечення; виявлення критичних і підкритичних ситуацій; сповіщення про стан безпеки; планування і забезпечення безперервності робочого процесу; відновлення при аварійних ситуаціях; інформаційна підтримка з питань безпеки).

Вибір СПЗ для захисту КМ будемо здійснювати за наступними критеріями: середовище функціонування; виконувані функції; вартість; вимоги до апаратного забезпечення; ефективність; умови розповсюдження.

Прийняття рішення щодо вибору певної компоновки СПЗ для захисту КМ будемо здійснювати за максимальною бальною оцінкою певної компоновки серед можливих варіантів компоновки з врахуванням можливості дублювання і резервування окремих функцій.

Розроблена методика базується на інформаційній моделі рис.1 [8] і містить 11 етапів.

Етап 1. Визначення актуальних загроз інформації для об'єкта захисту. Загрози виникають в разі наявності вразливостей в системі, можуть порушувати певні властивості захищеності інформації і, відповідно, можуть бути віднесені до одного із стандартних типів (К, Ц, Д, КЦ, КД, ЦД, КЦД [8]); характеризуються ймовірністю появи загрози і ймовірністю успішної реалізації загрози. Ймовірність появи загрози визначається як добуток ймовірності атаки на галузь застосування об'єкта захисту і ймовірності атаки певного типу. Ймовірність успішної реалізації загрози залежить від наявності у КЗЗ певних засобів протидії загрозі і ефективності їх роботи.

Етап 2. Визначення нормативних вимог до послуг безпеки. Реалізується в двох варіантах – для відомого і невідомого профілю захищеності.

Етап 3. Формування переліку вимог користувача до послуг безпеки і структури системи захисту.

Етап 4. Формування ранжованого за важливістю переліку функцій КЗЗ, який має протидіяти множині актуальних загроз інформації за допомогою СПЗ, із визначеними граничними значеннями показників якості їх виконання.

Етап 5. Вибір критеріїв оцінювання якості компоновки СПЗ і обчислення за методом попарних порівнянь вектору їх пріоритетів.

Етап 6. Оцінювання окремих СПЗ на відповідність функціональним вимогам.

Етап 7. Формування варіантів компоновки СПЗ з врахуванням багатошарової структури системи захисту, дублювання і резервування функцій КЗЗ.

Етап 8. Оцінювання варіантів компоновки СПЗ за визначеними на етапі 4 критеріями якості з врахуванням підвищення ефективності КЗЗ в разі функціонального резервування на одному рівні захисту і дублювання функцій різних засобів захисту на різних рівнях.

Етап 9. Відтинання варіантів, які не відповідають визначеним граничним значенням показників якості. Формування списку варіантів компоновки СПЗ, які відповідають граничним вимогам.

Етап 10. Оцінювання компоновок СПЗ із списку варіантів, визначеними на етапі 9, за критеріями, визначеними на етапі 5.

Етап 11. Вибір оптимальної компоновки СПЗ. Візуалізація результатів.

Висновки

В даній роботі проведено на основі аналізу нормативно-правової бази побудови захищених КМ визначені основні вимоги до спектру функцій КЗЗ, критерії вибору СПЗ для захисту КМ і методи прийняття рішень, на основі яких розроблена методика ефективної компоновки СПЗ для захисту КМ

Список літератури:

1. Jankowski D., Amanowicz M. On Efficiency of Selected Machine Learning Algorithms for Intrusion Detection in Software Defined Networks //INTL JOURNAL OF ELECTRONICS AND TELECOMMUNICATIONS, 2016, – VOL. 62,- № 3, – PP. 247-252

2. Husák M., J. Komárková J., Bou-Harb E., Čeleda P. Survey of Attack Projection, Prediction, and Forecasting in Cyber Security // IEEE Communications Surveys & Tutorials. – 2019. – Vol.21. – Issue 1. – PP.640–660. [URL]: https://www. researchgate. net/ publication/327449459_Survey_of_Attack_ Projection_ Prediction_and_Forecasting_in_Cyber_Security.

3. Гвоздьов Р. Ю. Метод і методика формального проектування комплексної системи захисту інформації в інформаційно-телекомунікаційних системах / Р. Ю. Гвоздьов, Р. В. Олійников // Радіотехніка. – 2020. – Вип. 203. – С. 91-96.

4. Кононова В. О. Оцінка засобів захисту інформаційних ресурсів / В. О. Кононова, О. В. Харкянен, С. В. Грибков // Вісник Національного університету "Львівська політехніка". Комп'ютерні системи та мережі. – 2014. – № 806. – С. 99-104.

5. Левченко М.П. Перспективи технології Honeypot, як засібу виявлення та дослідження атак // Матеріали VIII Всеукраїнської науково-технічної конференції з міжнародною участю «Сучасні проблеми інформаційної безпеки на транспорті».-Миколаїв: НУК, 2018 – С.130 – 133.

6. Проєкт I-CYBER. URL: https://icdc.gov.ua/diyalnist/projects/realizovani-u-2020-roci/proyekt-i-cyber

7. Турти М. Методика оптимізації систем захисту периметра // Матеріали 8-ої Міжнародної науково-технічної конференції «Інформаційні системи та технології ІСТ-2019». 9-14 вересня 2019 р. Харків – Коблеве. – Харків: ХНУРЕ, 2019. – С.254-259.

8. Турти М., Гратій А. Методика вибору спеціалізованого програмного забезпечення для захисту комп'ютерних мереж // Матеріали 9-ої Міжнародної науково-технічної конференції «Інформаційні системи та технології ІСТ-2020». – Харків: ХНУРЕ, 2020. – С.262-266.

УДК 62-519:004.931

ТЕХНОЛОГІЇ КОМП'ЮТЕРНОГО ЗОРУ В СИСТЕМАХ «РОЗУМНІЙ БУДИНОК»

Автор: *Дідківський О.О., магістрант, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

Науковий керівник: *Блінцов О.В., д.т.н., Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

З розвитком і доступністю технологій в сфері мікроконтролерів і програмного забезпечення в наш час все більш набуває попит на систему «Розумний дім», яка за допомогою високотехнологічних датчиків і пристроїв робить життя власника зручним у повсякденних задачах.

Система «Розумний дім» (*розумний будинок/ smart home, digital house*) – система домашніх пристроїв, здатних виконувати дії і вирішувати певні повсякденні завдання без участі людини. Функціонально пов'язуються між собою усі електроприлади будівлі, якими можна керувати централізовано – з пульта-дисплею. Прилади можуть бути під'єднані до комп'ютерної мережі, що дозволяє керувати ними за допомогою ПК та надає віддалений доступ до них через Інтернет. Завдяки інтеграції інформаційних технологій у домашні умови, усі системи та прилади узгоджують виконання функцій між собою, порівнюючи задані програми та зовнішні показники (обстановки).[1]

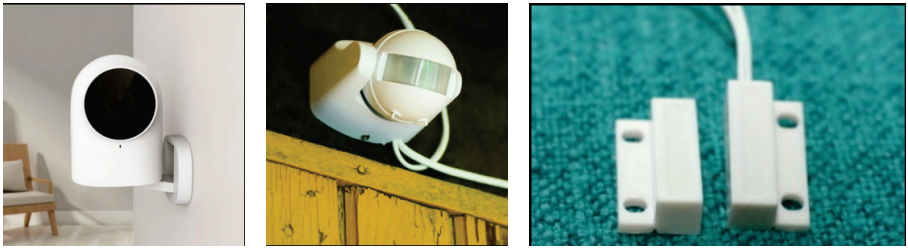
Система «Розумний дім» створюється за допомогою професійного проектування та програмування компаніями, що займаються розробкою проектів smart-home. Програми, що вводяться до алгоритмів multi-room розумного дому, розраховані на певні потреби мешканців

та ситуації, пов'язані із зміною середовища або безпекою. Особливістю smart-home є керування за допомогою пульта, на котрому людина може натиснути одну-єдину клавішу для створення певної обстановки. При цьому, сама система мульти-рум аналізує навколишню ситуацію та параметри усередині приміщення, та, керуючись власними висновками, виконує задані користувачем команди із відповідними налаштуваннями. Окрім того, електронні побутові прилади, встановлені у розумному будинку, можуть бути об'єднані у домашню Universal Plug'n'Play – мережу із виходом до інтернету.

За допомогою системи «розумного будинку» можна регулювати або включати світло в будь-якій з кімнат, перебуваючи поза домом, запускати прилади такі як, кондиціонер або систуму «Тепла підлога» до приходу власника, отримувати інформацію про людей або домашніх тварин, які знаходяться у будинку, а також бути в курсі будь-яких позаштатних ситуацій на кшталт поломки побутових приладів або задимлення приміщення.

Незважаючи на різне виконання, системи «розумного будинку» різних виробників мають схожі риси і функціонують за єдиними правилами.

До підсистеми охоронної сигналізації можуть входити такі прилади: камери відеоспостереження, датчики руху і відкривання дверей, тощо (рис 1) [2].



а б в

Рис. 1: а – камера відеоспостереження, б – датчик руху, в – датчик відкривання дверей

Перспективним вбачається застосування технологій комп’ютерного зору в системах «Розумний будинок», зокрема, при вирішення задач підсистеми охоронної сигналізації. Комп'ютерний зір – це область комп'ютерних наук, яка прагне розширити можливості комп'ютерів з ідентифікації та визначення об'єктів та людей на зображеннях та відео. Як і інші типи штучного інтелекту, комп'ютерний зір орієнтовано на виконання і автоматизацію завдань, які імітують людські можливості. У цьому випадку комп'ютерний зір намагається імітувати зір та сприйняття людини.

Основним компонентом ком’ютерного зору є сенсорний пристрій, який створює зображення. Сенсорний пристрій часто є просто фотокамерою, але може бути відеокамерою, пристроєм медичної візуалізації або будь-яким іншим пристроєм, що створює зображення для аналізу. Зображення потім надсилається на пристрій для аналізу. Пристрій для аналізу використовує можливості розпізнавання зображень для розбиття зображення на окремі частини порівняння знайдених образів з бібліотекою відомих образів та їх зіставлення. Образом може бути щось спільне, наприклад зовнішній вигляд об'єкта певного типу. Користувач запитує певну інформацію про зображення, а пристрій для аналізу надає такі відомості за результатами аналізу зображення [3].

Висновок. Перспективною вбачається інтеграція до підсистем охоронної сигналізації «Розумного будинку» спеціалізованого програмного забезпечення розпізнавання образів для виявлення порушників засобами відеоспостереження. Це дасть змогу комплексувати показання датчиків і зменшити ймовірність виникнення помилок першого та другого роду.

Список літератури:

1. Система «Розумний будинок» – https://ru.wikipedia.org/wiki/Домашняя_автоматизация
2. Огляд «Розумний будинок» – https://smarthomegadget.ru/umnyj-dom/
3. Комп’ютерний зір – https://azure.microsoft.com/ru-ru/overview/what-is-computer-vision/

УДК 004.832.34:004.056.52

ЗАХИСТ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНІЙ СИСТЕМІ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ

Автор: *Дмитриченко Г.Б., магістрант, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*
Науковий керівник: *Нужний С.М., к.т.н., доцент, зав. каф. КТІБ, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

Анотація**:** У цієї статті визначено проблемні питання забезпечення інформаційної безпеки в ІТС спеціального призначення, запропоновано оптимальні методи та засоби захисту інформації в ІТС спеціального призначення.

Вступ: Різке зростання великої кількості різноманітних інформаційних та інформаційно-телекомунікаційних систем в Україні обумовлено інтенсивним впровадженням сучасних інформаційних технологій. Широкі можливості обробки даних в автоматизованих системах забезпечують накопичення інформації з різних сфер життєдіяльності держави і суспільства, в тому числі конфіденційної інформації, що є власністю як юридичних так і фізичних осіб. Разом с тим зростає і небезпека несанкціонованого втручання в роботу цих автоматизованих систем. Важливість постановки та вирішення проблеми забезпечення безпеки сучасних інформаційних технологій обумовлюється необхідністю уточнення та обґрунтування достатності застосовуваних заходів захисту інформації, оптимізації систем захисту, підвищення ефективності контролю безпеки інформації.

Мета: Розгляд особливостей функціонування ІТС спеціального призначення та побудова моделей створення захищеної інформаційної системи спеціального призначення.

Основна частина: Враховуючи особливості функціонування ІТС спеціального призначення, відомості, що оброблюються в цій системі, за правовим режимом доступу поділяються на відкриту інформацію та

інформацію з обмеженим доступом (державна таємниця, службова інформація, конфіденційна інформація, тощо).

Відкрита інформація може бути доступна авторизованим користувачам на безоплатній основі на офіційному веб-порталі центрального органу виконавчої влади, що забезпечує реалізацію державної політики у відповідній сфері.

Всі відомості, внесені до відомчої ІТС спеціального призначення, повинні захищатись відповідно до вимог законодавства у сфері захисту інформації. Для забезпечення захисту інформації в ІТС під час її обробки, зберігання та передачі каналами зв’язку законодавством України передбачено створення комплексної системи захисту інформації (КСЗІ) з підтвердженою відповідністю. Підтвердження відповідності здійснюється за результатами державної експертизи в установленому законодавством порядку. Сукупність вжитих заходів із захисту інформації має забезпечувати конфіденційність, цілісність та належний порядок доступу до відомостей, внесених до ІТС спеціального призначення, а також захист інформації від витоку технічними каналами.

Впровадження відомчої ІТС спеціального призначення, як правило, здійснюється на двох рівнях (центральному та регіональному).

Автоматизована інформаційна система (АІС) центрального рівня виконує функції головного серверу та призначена для накопичення всіх даних від систем регіонального рівня, їх узагальнення та надання відповідного доступу для проведення аналітичної роботи. Побудова АІС центрального рівня здійснюється на базі серверів даних (основного та резервного), серверу адміністрування та безпеки, АРМ адміністраторів та АРМ користувачів, об'єднаних в локальну обчислювальну мережу (ЛОМ), підключену до захищеної мережі передачі даних.

Регіональний рівень передбачає встановлення клієнтської частини програмного забезпечення АІС в територіальних органах на АРМ, об'єднаних в ЛОМ. АРМ територіальних органів та віддалених підрозділів підключаються до центрального серверу за допомогою захищеної мережі передачі даних.

Таким чином, відомча ІТС спеціального призначення буде являти собою розподілену обчислювальну мережу, до складу якої входять наступні складові:

– захищена серверна зона вузла першого (центрального) рівня;

– ЛОМ вузла першого (центрального) рівня;
– ЛОМ вузлів другого (регіонального) рівня;
– мережеве та комутаційне обладнання;
– захищена транспортна мережа.

Передбачаються наступні режими функціонування компонентів системи:

– всі сервери захищеної серверної зони – цілодобово;
– робочі станції (РС) адміністраторів безпеки – цілодобово;
– РС системних адміністраторів та користувачів – протягом робочого дня.

Особливості функціонування ІТС спеціального призначення [1]:

– оброблення як відкритої інформації, так і інформації з обмеженим доступом;
– безперервний цілодобовий режим функціонування серверних компонентів та необхідність забезпечення дотримання заявленого часового регламенту оброблення запитів користувачів;
– використання для захисту інформації апаратно-програмних засобів, що мають позитивний експертний висновок (сертифікат відповідності);
– обов'язковість ідентифікації й автентифікації користувачів з використанням цифрового електронного підпису, захищеного електронного носія;
– необхідність криптографічного захисту інформації в мережах передачі даних.

З урахуванням особливостей архітектури, інформації, що обробляється, та технології її оброблення, згідно з НД ТЗІ 2.5-005-99 відомча ІТС спеціального призначенняслід відносити до автоматизованих систем класу "3" – розподілений багатомашинний багатокористувачевий комплекс, який обробляє інформацію різних категорій конфіденційності, з підвищеними вимогами до забезпечення конфіденційності, цілісності та доступності оброблюваної інформації [2].

Реалізація функцій захисту досягається шляхом використання об'єднаних в єдину систему вбудованих послуг безпеки операційних

систем серверів та робочих станцій, сертифікованих криптографічних та технічних засобів захисту, можливостей спеціалізованого і антивірусного програмного забезпечення, а також шляхом виконання спеціальних організаційних, інженерних та технологічних заходів із захисту інформації. Компоненти комплексу програмно-апаратних засобів ІТС, що беруть участь в реалізації політики безпеки інформації, є складовими КСЗІ в ІТС 2 [1].

При побудові захищених ІТС державних органів найбільш оптимальним вважається інтеграція її компонентів до Національної телекомунікаційної мережі (НТМ). НТМ створюється Держспецзв'язку відповідно до Указу Президента України від 13 лютого 2017 року №32/2017[3], функціонуватиме в інтересах органів державної влади і забезпечуватиме можливість отримання ними повного спектру сучасних телекомунікаційних сервісів. НТМ створюється на базі існуючих спеціальних телекомунікаційних систем (мереж) і комплексів технічних засобів, а також телекомунікаційних мереж спеціальних споживачів та відомчих мереж органів державної влади

Як першочергові слід зазначити завдання розробки наступних моделей:

- моделей визначення властивостей ІТС;
- моделей визначення загроз безпеки інформації в ІТС;
- моделей визначення типових уразливостей ІТС;
- моделей створення організаційного забезпечення побудови системи захисту в ІТС;
- моделей створення технічного забезпечення побудови системи захисту в ІТС;
- моделей управління заходами впровадження систем захисту інформації в ІТС;
- моделей перевірки відповідності впроваджених заходів нормативним документам із захисту інформації;
- моделей відновлення функціонування роботи ІТС.

Висновки: На основі аналізу особливостей функціонування ІТС спеціального призначення запропоновано засади розробки моделей організаційних та технічних заходів, які включають чотири основні групи моделей управління щодо:

– встановлення причин, які обумовлюють необхідність розробки захищеної ІТС;

– встановлення мети та задач її розробки;

– розробки і порівняльного аналізу варіантів реалізації системи захисту в ІТС;

– визначення відповідності заходів із захисту інформації нормативним документам.

Отримані моделі утворюють теоретичне підґрунтя у напрямку розробки заходів з побудови захищених ІТС спеціального призначення.

Список літератури:

1. Васєв В.О., Майданюк П.В. Типова модель захищеної інформаційно-телекомунікаційної системи // Збірник наукових праць VIII Всеукраїнської науково-практичної конференції "Стан та удосконалення безпеки інформаційно-телекомунікаційних систем (SITS'2016)". – Миколаїв: ДП НВКГ "Зоря-Машпроект", 2016. – с. 11-15.

2. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. Наказ Департаменту спеціальних телекомунікаційних систем та захисту інформації СБ України від 28.04.99 р. № 22. (НД ТЗІ 2.5-005-99).

3. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року "Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації": Указ Президента України від 13 лютого 2017 р. №32/2017. – [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/ laws/show/32/2017.

УДК 004.056.5

УДОСКОНАЛЕННЯ АЛГОРИТМУ ПОТОЧНОГО ШИФРУВАННЯ RC4

Автори: *Дюльдев В.О.; Михайлов М.М.; Пожидаев М.Г., Харківський національний економічний університет імені Семена Кузнеця, м. Харків, Україна*

Вступ. Поточний технологічний прогрес у світі та масова інформатизація змушує серйозно задуматися про захист даних, які підлягають інформатизації. Якщо система повинна виконувати функції конфіденційності, автентифікації, цілісності, а також завдань криптографічної обробки інформації, пов'язаних із забезпеченням цих послуг можна зробити висновок про те, що є необхідність використання спеціальних механізмів безпеки.

Дослідження показали, що для побудови механізмів безпеки інформації традиційно використовують методи криптографічного перетворення інформації, тобто шифрування.

Основна частина. Шифрування полягає в заміні, підстановці, по елементній операції над елементами відкритого тексту і секретного ключа. На практиці використовують дуже довгу псевдовипадкову послідовність, а шифрування здійснюють за правилом одноразового ключового блокнота. Вважаючи використовувану стрічку випадковою і нескінченною, реалізовану криптосистему вважають абсолютно стійкою.

Проведений аналіз сучасних механізмів криптографічного захисту інформації показав, що невід'ємною частиною будь-якої системи захисту інформації є генерація псевдовипадкової послідовності.

Алгоритм RC4 являє собою потоковий шифр зі змінною довжиною ключа. Він був розроблений у 1987 році Роном Рівестом для компанії RSA DataSecurity, Inc. На протязі 7 років цей шифр ліцензувався компанією тільки на умовах нерозголошення, однак в 1994 році він був анонімно опублікований в інтернеті і с тих пір став доступним для незалежного аналізу [1].

Алгоритм потокового шифрування RC4 складається з трьох частин:

- створення ключа;
- алгоритм шифрування;

– алгоритм розшифрування.

Ключ в RC4 представляє собою послідовність байтів довільної довжини, з якої будується початковий стан шифру S – перестановка усіх 256 байтів.

З початку S блок заповнюється послідовними значеннями від 0…255, потім кожний послідуючий елемент S блоку обмінюється місцями з елементом, номер якого визначається елементом ключа K, самим елементом та сумою номерів елементів, з якими виконується обмін на попередніх ітераціях. Псевдовипадкова послідовність розраховується за рахунок використання простих математичних операцій складання по модулю 256. На рисунку 1 представлений основний крок формування псевдовипадкової послідовності [2].

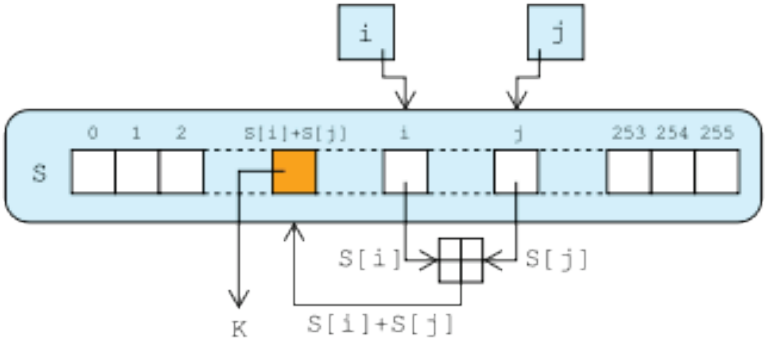


Рисунок 1. Формування псевдовипадкової послідовності алгоритму потокового шифрування RC4

При кожному формування псевдовипадкової послідовності i=0, j=0. В ході проведених досліджень були розроблені міні версій алгоритму потокового шифрування для поля $GF(2^3)$, $GF(2^4)$ тобто використовуються S – блоки S_0, S_1, S_2, S_3 та S_0, S_1, S_2,… S_{15} відповідно при всіх можливих комбінаціях i та j. Було встановлено, що існують такі значення i та j при яких генератор формує послідовності малого періоду. Так довжина періоду для поля $GF(2^3)$ складала 54, а для поля $GF(2^4)$ 240 елементів. Результати досліджень представлені в таблиці 1.

Таблиця 1 – Значення S-блоку та початкових елементів

Значення S-блоку																i	j	Довжина періоду	Розмірність поля
S_0	S_1	S_2	S_3	S_4	S_5	S_6	S_7	S_8	S_9	S_{10}	S_{11}	S_{12}	S_{13}	S_{14}	S_{15}				
0	2	7	5	4	1	3	6	-	-	-	-	-	-	-	-	4	5	56	$GF(2^3)$
7	0	6	1	2	3	4	5	-	-	-	-	-	-	-	-	2	3	56	$GF(2^3)$
1	2	4	6	7	3	5	8	10	11	12	13	0	14	9	15	15	0	240	$GF(2^4)$

В роботі запропоновано вдосконалену схему формування псевдовипадкових чисел, структурна схема якого представлена на рисунку 2.

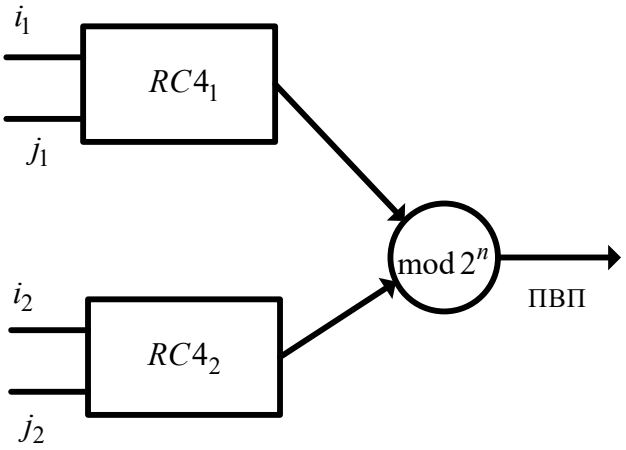


Рисунок 2. Структурна схема вдосконаленого генератора RC4

У якості функції ускладнення обрано складання по модулю 2^n де n розмірність поля. Введення ключів і та j які нерівні 0 дає змогу збільшити ключову послідовність, тобто ускладнити криптоаналіз.

Висновки. Проведені дослідження показали, що удосконалений генератор псведовипадкових чисел RC4 дозволяє швидко формувати псевдовипадкові послідовності в порівнянні з оригіналом та дає можливість збільшити кількість ключів (начальних станів), що ускладнює криптографічний аналіз та збільшує криптографічну стійкість. Також запропоновано збільшити розмірність поля $GF(2^n)$ де $n>10$. Використання збільшеного поля збільшить період сформованої послідовності.

Список літератури:

1. Корченко О.Г., Сіденко В.П., Дрейс Ю.О. Прикладна криптологія : системи шифрування : підручник / – К. : ДУТ, 2014. – 448 с.
2. https://ru.wikipedia.org/wiki/RC4

УДК 534.843.5

ОЦІНКА ВПЛИВУ РЕВЕРБЕРАЦІЇ НА РОЗБІРЛИВІСТЬ МОВИ, СПОТВОРЕНОЇ СТАЦІОНАРНИМ ШУМОМ

Автор: *Змієвець В.Р., магістрант, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

Науковий керівник: *Козирєв С.С., к.т.н., Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

На даний час актуальним є питання забезпечення розбірливості мови, оскільки стрімко розвиваються інформаційно-керуючі комплекси, в яких використовується дистанційне керування пристроями за допомогою голосу. Тому особливої важливості набувають системи розпізнавання мовної інформації, що вбудовуються в такі пристрої. Важливим також є забезпечення розбірливого та якісного мовного сигналу для телефонних розмов, для військових ліній зв'язку. Актуальним є питання захисту приміщень від витоку інформації. В таких випадках сигнал на виході маскується чи глушиться. Тому на сьогоднішній день існує велика кількість різних систем активного віброакус-

тичного маскування мовної інформації, які створюють акустичні завади у вигляді стаціонарних та нестаціонарних шумів. Для оцінювання захищеності мовної інформації набуває широкого вжитку критерій розбірливості мови. Такий критерій більш точно відображає сприйняття смислової складової мовного повідомлення й ефективність прийнятих заходів захисту мовної інформації від існуючих загроз у порівнянні з критерієм відношення сигнал/шум (SNR) [1].

Існують ситуації, які вимагають знаходження шляхів, щодо підвищення розбірливості мовного сигналу, виходячи з умов приміщення. Відомим є те, що реверберація вносить зміни до сигналу [2]. Загальновідомо що пізня реверберація вносить спотворення, які знижують розбірливість мови, тому її намагаються усунути. Рання реверберація, чи ранні відбиття, можуть сприяти зростанню розбірливості, оскільки приходитимуть синфазно, тобто первинний сигнал буде підсилений своїм же відбиттям, що покращить розбірливість мови за рахунок збільшення відношення сигнал-завада. Але цей ефект залежить від характеристик приміщення, тому існують умови, що призводять до погіршення розбірливості при наявності ранньої реверберації.

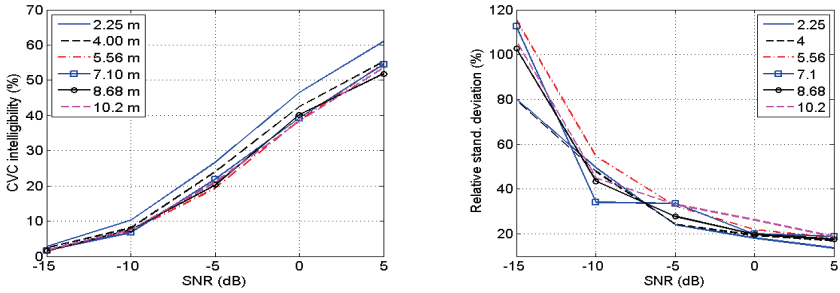
Метою роботи даної роботи є проведення оцінки розбірливості мови в приміщеннях в умовах дії завад у вигляді білого шуму та реверберації, а також дослідження впливу ранньої реверберації, тобто ранніх відбиттів, на розбірливість мови, що спотворюється стаціонарними шумами.

Найбільш вагомі результати з оцінювання розбірливості мови в приміщеннях було отримано Бредлі та Арвейлер в період з 2003 по 2013 роки [3, 4]. Так всі досліди показали, що бінауральне прослуховування дає більший виграш для розбірливості. Було підтверджено важливість ранніх відбиттів. Також було показано, що ранні відбиття підвищують розбірливість в умовах маскування мовного сигналу. Найкращий ефект маскування показали стаціонарні шуми. Але їх експерименти не оцінювали вплив реальних імпульсних характеристик приміщень на розбірливість в умовах маскування мовного сигналу.

Існує два підходи до оцінювання якості та розбірливості мовних акустичних сигналів: суб'єктивний та об'єктивний. Необхідно враховувати, що в багатьох об'єктивних методах використовуються експериментальні результати, які були отримані в процесі суб'єктивних артикуляційних випробувань.

До об'єктивних відносяться методи, які базуються на інструментальних вимірюваннях параметрів мовних повідомлень, до суб'єктивних – методи, основані на безпосередній експертній оцінці. Варто зазначити недоліки суб'єктивних методів: низька оперативність, трудомісткість, складність отримання результатів. При цьому їх беззаперечною перевагою (наприклад, методу артикуляційних випробувань) є висока достовірність результатів, одержаних людьми, оскільки саме людина є кінцевим споживачем мовних сигналів. Об'єктивні методи є значно швидшими та дешевшими у порівнянні з суб'єктивними. В [5] запропоновано програмну систему суб'єктивного оцінювання розбірливості мови, спотвореної стаціонарним шумом та реверберацією, яка поєднує переваги суб'єктивного та об'єктивного методів оцінювання розбірливості мови.

В результаті використання даної методики при дослідженні розбірливості мови в приміщеннях, в умовах дії завад у вигляді білого шуму та реверберації, отримано наступні результати. Оцінку розбірливості мови, спотвореної білим шумом та реверберацією, наведено на рис. 1 а. На рис. 1 б наведено відносне стандартне відхилення цього результату.



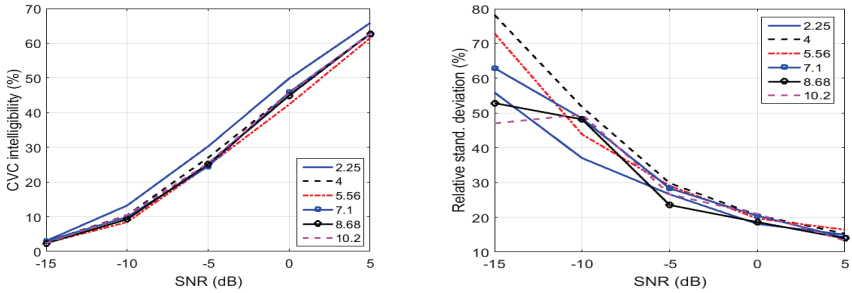
а б

Рис. 1. Оцінки розбірливості мови (а) та їх відносне стандартне відхилення (б)

Наведені результати свідчать, що при фіксованих відношеннях сигнал-шум, розбірливість мови є найвищою для відстані 2,25 м, на

відстані 4,00 м розбірливість є помітно меншою, а для більших дистанцій розбірливість є практично однаковою та найменшою.

Отримані результати підтверджують шкідливу дію пізньої реверберації. Для перевірки впливу ранньої реверберації було вирішено не враховувати (відтяти) в імпульсних характеристиках «хвости», що починаються після 50 мс, та повторити експериментальні дослідження розбірливості мовних сигналів. Результати повторного оцінювання розбірливості мови наведено на рис. 2 а, а на рис. 2 б наведено відносне стандартне відхилення цього результату.



а б

Рис. 2. Оцінки розбірливості мови (а) та їх відносне стандартне відхилення (б) в умовах відсутності пізньої реверберації

Відкидання «хвостів» імпульсних характеристик призвело до незначного 3-5% в діапазоні SNR = -5…+5 дБ, проте помітного підвищення розбірливості мови. Цей результат є очікуваним, оскільки відомо про шкідливу дію пізньої реверберації.

Проте виявився, що ранні відбиття також погіршують розбірливість мови. Це погіршення сягає 5-8% в діапазоні SNR = – 5…+5 дБ (рис. 2 а). Причиною цього може бути те, що очікуване підсилення рівня сигналу за рахунок ранніх відбиттів компенсується спотворенням форми сигналу, спричиненим нерівномірністю АЧХ кімнати для випадку дії ранніх відбиттів. Тобто, в даному випадку розбірливість знижується через зниження якості сигналу, й це зниження переважає над збільшенням розбірливості за рахунок збільшення відношення сигнал-шум, обумовленого ранньою реверберацією.

Таке припущення підтверджується аналітичною моделлю, коли на прямий звук (в даному випадку це гармонічний сигнал) накладається одне раннє відбиття:

$$y(t) = \cos(w_0 t) + q\cos\left[w_0(t - t_0).\right]$$

Амплітуда результуючого коливання залежить не тільки від амплітуди раннього відбиття та часу затримки, але й від частоти гармонічного сигналу:

$$A_y = \sqrt{1 + q^2 + 2q\cos w_0 t_{0,}}$$

тобто наявність раннього відбиття еквівалентне дії «гребінчастого фільтру», який на певних частотах підсилює сигнал, а на певних – послаблює.

Розглянута модель дозволяє пояснити причину погіршення якості мовного сигналу через дію ранніх відбиттів та, як наслідок, погіршення розбірливості мови.

Висновки. Результати дослідження показали, що на розбірливість мови впливає як пізня так і рання реверберація. Зі зростанням відстані розбірливість знижується в основному із-за шкідливої дії пізньої реверберації. Проте після видалення «хвостів» імпульсних характеристик виявилося, що ранні відбиття також знижують розбірливість мови, порівняно з прямим звуком. Це явище спричинене нерівномірністю АЧХ приміщень, які можна розглядати як фільтри, що й спричиняють зниження якості та розбірливості мовного сигналу. Для врахування впливу на розбірливість мовного сигналу необхідно мати імпульсні характеристики досліджуваних приміщень.

Список літератури:

1. Хорев А.А. Методы защиты речевой информации и оценки их эффективности / А.А. Хорев, Ю.К. Макаров // Защита информации. Конфидент. – 2001. – № 4. – С. 22-33.

2. Акустическая экспертиза каналов речевой коммуникации. Монография / Дидковский В.С., Дидковская М.В., Продеус А.Н. – Киев: Имэкс-ЛТД, 2008. – 420 с.

3. Bradley, J. S., Sato, H., and Picard, M. (2003). "On the importance of early reflections for speech in rooms," J. Acoust. Soc. Am. 113, 3233-3244.

4. Iris Arweiler, Jorg M. Buchholz, Torsten Dau (2009). "Speech intelligibility enhancement by early reflections", https://proceedings.isaar.eu/index.php/isaarproc/article/view/2009-29.

5. Продеус А.М. Суб'єктивне оцінювання розбірливості мови на тлі шуму та реверберації. "Мікросистеми, електроніка та акустика", том 23, № 2, 2018, с. 66-73.

УДК 004.056.5: 534.843

ВПЛИВ РІВНЯ МОВЛЕННЄВОГО СИГНАЛУ НА ЗАЛЕЖНІСТЬ РОЗБІРЛИВОСТІ МОВИ ВІД ВІДНОШЕННЯ СИГНАЛ/ШУМ

Автори: *Касьянов Ю.І., старший викладач; Золотченко В.В., студентка; Іванова А.В., студентка; Іванов В.І., студент, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

Вступ. Мова є основним способом комунікації між людьми. Тому доля мовної інформації в інформаційних потоках завжди була і буде дуже високою, а її захист є першочерговою задачею при побудові будь-якої системи технічного захисту інформації на об'єктах інформаційної діяльності. Побудова системи захисту мовної інформації починається і закінчується оцінюванням ступеня її захищеності. При цьому останнім часом в провідних країнах світу для оцінювання і нормування захищеності мовної інформації використовують критерій розбірливості мови.

Основною характеристикою, що дає можливість оцінити ефективність тих чи інших активних засобів захисту, є залежність розбірливості мови від відношення сигнал/шум.

В ряді наукових робіт доведено, що ця характеристика залежить від виду завади [1-5]. Причому, при розрахунку цієї характеристики використовуються емпіричні характеристики мови отримані при досить високих рівнях мовного сигналу [6]. Однак інформативні сигнали в акустичних каналах витоку мовної інформації мають досить малі

рівні. В той же час відомостей щодо залежності даної характеристики від рівня мовного (інформативного) сигналу в літературі не виявлено.

Метою роботи є дослідження впливу рівня інформативного мовного сигналу на залежність розбірливості мови від відношення сигнал/шум.

Основна частина. Щоб врахувати максимум факторів, що впливають на розбірливість мови, для дослідження було обрано суб'єктивний метод артикуляційних випробувань [6-8], який є найбільш універсальним і точним.

Було розроблено методику дослідження. Основні стадії експерименту наведено на рис.1.

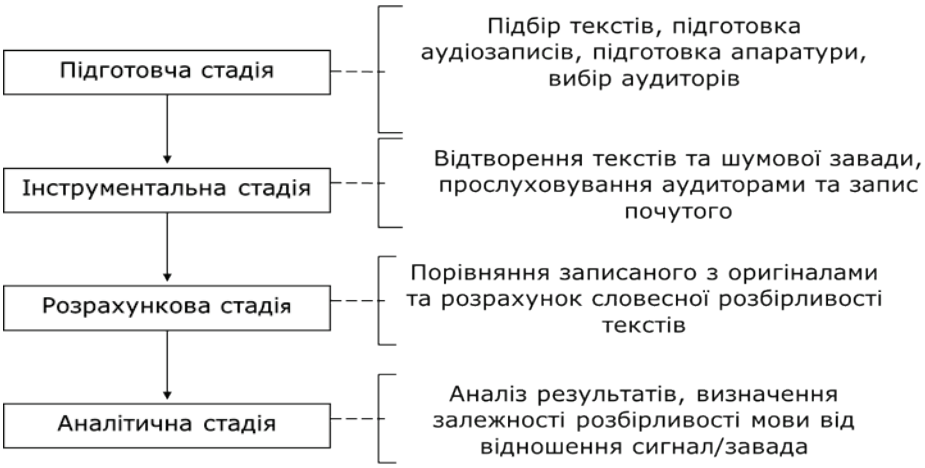


Рисунок 1 – Основні стадії експерименту

Програма досліджень включає підготовку фонограм артикуляційних таблиць слів, їх відтворення при різних рівнях мовного сигналу і різних рівнях завади та прослуховування аудиторами з записом почутого, визначення словесної розбірливості для кожного режиму і для кожного аудитора, статистичну обробку ре-

зультатів та визначення усереднених залежностей розбірливості мови від відношення сигнал/шум.

В якості тестового матеріалу використовувалися артикуляційні таблиці з 50 слів, взяті з ГОСТ 16600-72 [7].

Для запису фонограм використано персональний комп'ютер та програму Sound Forge. Диктори читали слова рівним голосом, з постійним рівнем мови, чітко без підкреслювання окремих звуків. Темп зачитування слів: 15…20 слів за хвилину з паузами між словами 2…4 секунди для їх запису аудиторами. Запис проводився у форматі нетисненого цифрового звуку Wav (44000 Гц, 16 біт, моно). Для запису використовувався електродинамічний мікрофон SHURE C606.

Інструментально-вимірювальна стадія експерименту проводилась в лабораторії захисту аудіо і відеоінформації кафедри комп'ютерних технологій та інформаційної безпеки. Схема експерименту представлена на рис. 2.

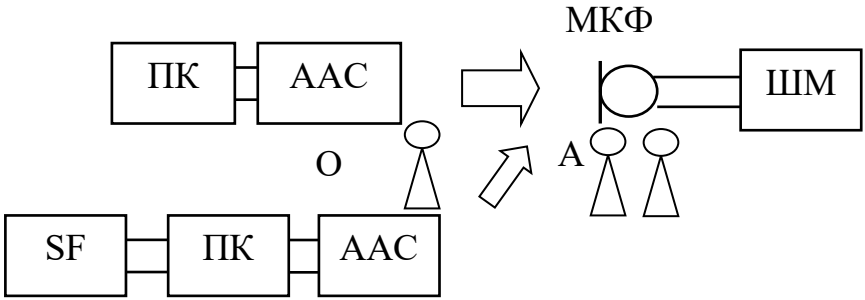


Рисунок 2 – Схема експерименту: ПК – персональний комп'ютер; SF – програма Sound Forge; МКФ – вимірювальний мікрофон; А – аудитори; О – оператор; ШМ – шумомір; ААС – активна акустична система

В експерименті приймали участь 4 аудитори, які є студентами, що навчаються за спеціальністю 125 – "Кібербезпека" та викладач, що виконував функції оператора.

Підготовлені звукові файли відтворювались програмою Sound Forge 10.0 на ПК і через звукову карту Realtek High Definition Audio сигнал подавався на активну акустичну систему Primax Soundstorm (потужністю 14 Вт, номінальний діапазон частот 50…18000 Гц). Для зниження похибки, що вноситься відтворювальною апаратурою, проводилось попереднє налаштування АЧХ каналу відтворення, щоб вона була максимально плоскою.

Сигнал шумової завади представляв собою сигнал «білого» шуму, згенерований в програмі обробки звуку Sound Forge та виведений через звукову карту на акустичну систему.

Дослідження проводились при рівнях мовного сигналу 44 і 64 дБ та відношеннях сигнал/шум -10; -5; 0; 5; 10 дБ, що задавались зміною рівня шуму. Вимірювання рівнів сигналу та шуму в октавних смугах з середньогеометричними частотами 125; 250; 500; 1000; 2000; 4000; 8000 Гц виконувалось шумоміром ВШВ-003 з конденсаторним мікрофоном. Вимірювання проводилися в режимі «повільний».

При одночасному відтворенні інформативного сигналу та шумової завади, аудитори слухали та записували відтворені слова з артикуляційних таблиць. Дана процедура повторювалась від 3 до 5 разів, після чого робилась перерва на відновлення слухової системи. Перед прослуховуванням проводилась попередня адаптація аудиторів до шуму на протязі 5…7 хвилин.

В результаті проведення експерименту було отримано 40 записів від 4 аудиторів.

Обробка результатів проводилась шляхом порівняння записаного з оригіналами артикуляційних таблиць та розрахунком розбірливості мови для кожного аудитора і кожного режиму, як відношення правильно сприйнятих слів до загальної кількості в артикуляційній таблиці. Далі було проведено усереднення значень словесної розбірливості для кожного режиму.

За даними експериментів побудовано графіки залежності словесної розбірливості мови від відношення сигнал/шум (рис.3.).

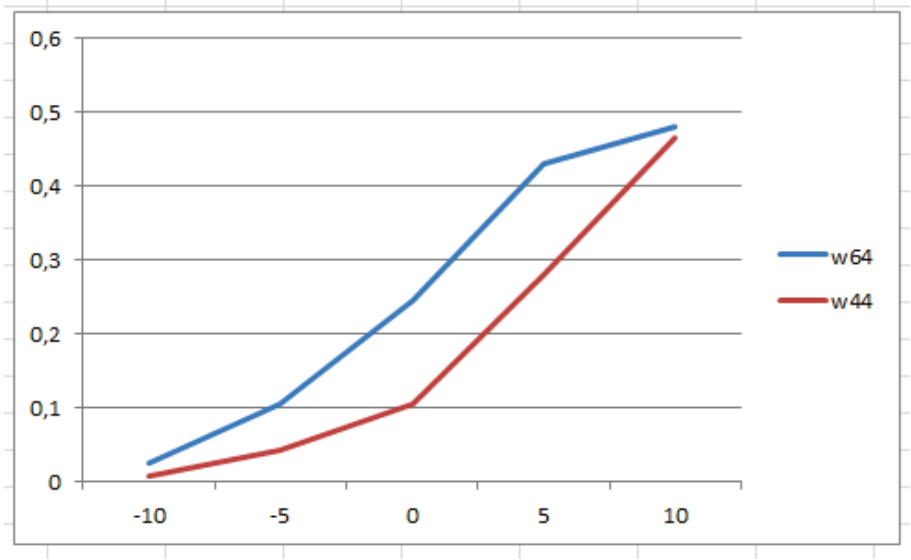


Рисунок 3 – Графік залежності словесної розбірливості від відношення сигнал/шум при різних рівнях мовного сигналу

Як бачимо, рівень мовного (інформативного) сигналу впливає на характер залежності розбірливості мови від відношення сигнал/шум. Причому цей вплив найбільше виражений при сумірності інформативного сигналу і шумової завади. При збільшені та зменшенні відношення сигнал/шум цей вплив зменшується.

Висновок:

1. Рівень інформативного мовного сигналу впливає на характер залежності розбірливості мови від відношення сигнал/шум, що вказує на необхідність проводити дослідження ефективності засобів захисту мовної інформації при робочих рівнях інформативного сигналу в точках можливого знімання інформації (контрольних точках).

2. Доцільно провести уточнюючі дослідження з більшою кількістю рівнів сигналу.

Список літератури:

1. Хорев А.А. (2001) Методы защиты речевой информации и оценки их эффективности. Специальная техника, № 4, С. 22 – 33.

2. Дидковский В.С., Дидковская М.В., Продеус А.Н. (2008) Акустическая экспертиза каналов речевой коммуникации. Монография. Киев, Имэкс-ЛТД, 420 с.

3. Касьянов Ю.І., Нужний С.М. (2016) Оцінювання ефективності генератора реальної мовоподібної завади за критерієм розбірливості мови. Вісник Нац. ун-ту "Львівська політехніка": Автоматика вимірювання та керування, №.852, С. 105 – 110.

4. Volodymyr Blintsov, Sergey Nuzhniy, Yurii Kasianov, Viktor Korytskyi (2019) Development of a mathematical model of scrambler-type speech-like interference generator for system of prevent speech information from leaking via acoustic and vibration channels. Technology audit and production reserves, № 5/2(49), p. 19–26. DOI: 10.15587/2312-8372.2019.85133

5. Трушин В.А., Иванов А.В., Рева И.Л. (2016) О корректировке методики оценки защищённости речевой информации от утечки по техническим каналам. Специальная техника, № 6, С. 22–30.

6. Покровский Н.Б. (1962) Расчет и измерение разборчивости речи. Москва, Гос. изд-во литературы по вопросам связи и радио, 392 с.

7. Передача речи по трактам радиотелефонной связи. Требования к разборчивости речи и методы артикуляционных измерений: ГОСТ 16600-72. – М.: ИПК Издательство стандартов, 1973. – 90 с.

8. Передача речи по трактам связи. Методы оценки качества, разборчивости и узнаваемости : ГОСТ Р 50840-95. – М.: Госстандарт Росии, 1997.

УДК 004.056.53: 534.781

ЩОДО ТЕКСТОВОГО МАТЕРІАЛУ ПРИ ДОСЛІДЖЕННІ УЗАГАЛЬНЕНИХ СПЕКТРІВ МОВЛЕННЄВОГО СИГНАЛУ

Автори: *Касьянов Ю.І., старший викладач; Хівріч В.В., студентка; Михайличенко А.В., студентка; Трощенко С.С., студент, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

Вступ. Незважаючи на те, що інформаційні потоки все більше зміщуються в область комп'ютерних та телекомунікаційних систем, доля акустичної мовної інформації в інформаційних потоках суден та об'єктів морської інфраструктури, особливо в оперативній передачі конфіденційної інформації та команд керування, залишається значною. Це обумовлено тим, що мова є природнім і найбільш розповсюдженим способом обміну інформацією між людьми та несе велике смислове навантаження.

Враховуючи, що наразі існує широкий арсенал портативних засобів акустичної мовної розвідки, захист мовної інформації є одним з найважливіших завдань у загальному комплексі заходів щодо забезпечення інформаційної безпеки об'єктів водного транспорту. Заходи щодо технічного захисту мовної інформації починаються і закінчуються оцінюванням ступеня її захищеності від витоку технічними каналами.

На протязі тривалого часу критерієм захищеності мовної інформації було відношення сигнал/шум в контрольних точках (точках можливого знімання інформації). В Україні цей критерій використовується і сьогодні. Однак, цей критерій є неінваріантним щодо виду шумової завади [1-4], що стримує впровадження в практику ефективних генераторів реальних мовоподібних завад. Тому наразі в ряді провідних країн світу в якості критерію захищеності взято словесну розбірливість перехопленого мовного повідомлення, яка є безпосередньою мірою зрозумілості. Впровадження даного критерію в Україні видається лише питанням часу [5].

Основним методам визначення розбірливості мови в сертифікованих методах оцінювання захищеності мовної інформації за даним критерієм є формантний метод та його модифікації. При цьому вико-

ристовуються спектральні характеристики мови – спектр довготривалої мови та розподіл формант у мовному діапазоні частот [1, 6].

Враховуючи, що в службових інформаційних потоках українських об'єктів інформаційної діяльності, в тому числі на водному транспорті, суттєво зріс об'єм інформації українською мовою, дослідження спектральних характеристик української мови та їх використання в оцінюванні захищеності мовної інформації за критерієм розбірливості наразі є актуальною задачею.

Метою роботи є експериментальне визначення узагальненого спектру довготривалого українського мовленнєвого сигналу за октавними рівнями для використання в формантному методі при оцінюванні захищеності мовної інформації за критерієм розбірливості.

Основна частина. Дослідження в цьому напрямку та їх результати описані в [7, 8]. Однак там для аналізу взято фонограми українських мовленнєвих сигналів з телевізійних новин, що може приводити до суттєвих інструментальних похибок, обумовлених налаштуваннями студійної апаратури та апаратури передачі і прийому телевізійних сигналів. В описаних нижче дослідженнях для аналізу використовувались фонограми безпосередньо "живих" дикторських голосів.

Було розроблено методику проведення експерименту, що складається з 4-х етапів: підготовчий, інструментально-вимірювальний, розрахунковий і аналітичний (рис.1).

На підготовчому етапі були записані аудіо файли українською мовою тривалістю по 15 секунд, що відповідає вимозі довготривалої мови, при читанні тексту двома групами дикторів: чоловіків і жінок. Кожна група складалася з трьох дикторів. Кожен диктор зачитував 3 різних тексти неоднорідного характеру. В якості мовного матеріалу використовувалися художні та публіцистичні тексти. Для запису мовних сигналів використовувався електродинамічний мікрофон HIGH SENSITIVE MIC AH59-01198E. Запис проводився на ноутбуці MacBook Air, програмою Real Pad у форматі не стисненого цифрового звуку Wav (44000 Гц, 16 біт). Нерівномірність АЧХ звукової карти в мовному діапазоні частот не перевищувала 0,3 дБ за результатами тестування програмою RightMark Audio Analyzer.

Рисунок 1 – Основні етапи експерименту

На інструментально-вимірювальному етапі підготовлені звукові файли відтворювались програмою Sound Forge на персональному комп'ютері (ПК) і через звукову карту Realtek High Definition Audio сигнал подавався на активну акустичну систему (ААС) Primax Soundstorm (рис.2). Вимірювання рівнів сигналу в октавних смугах з середньогеометричними частотами 125; 250; 500; 1000; 2000; 4000; 8000 Гц виконувалось шумоміром ВШВ-003 з конденсаторним мікрофоном в режимі «повільний». Відстань між ААС і мікрофоном шумоміра було встановлено 0,25 м, щоб мінімізувати вплив відбитого звуку на результат.

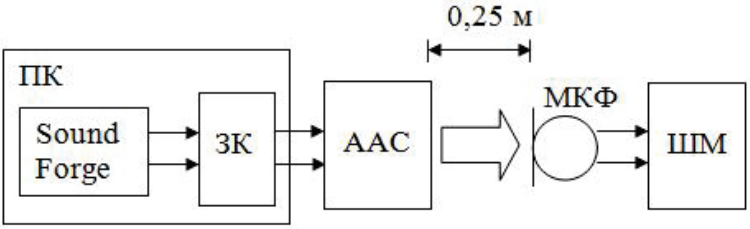


Рисунок 2 – Схема експериментальної установки: ПК – персональний комп'ютер; ЗК – звукова карта; ААС – активна акустична система; МКФ – мікрофон; ШМ – шумомір

Звучання усіх фонограм перед проведенням вимірювань в октавних смугах регуляторами гучності приводились до однакового інтегрального рівня звукового тиску в 70 дБ, що забезпечило перевищення рівня мовного сигналу над рівнем фонового шуму не менше 20 дБ. Для мінімізації похибки вимірювань попередньо було проведено налаштування максимально плоскої АЧХ каналу відтворення.

Отримані усереднені спектри жіночих та чоловічих голосів і узагальнений спектр українського мовленнєвого сигналу наведено на рис. 3. Порівняно зі спектром, отриманим при аналізі фонограм телевізійних новин [8], октавний рівень в смузі з середньогеометричною частотою 8000 Гц приблизно на 9 дБ нижчий. Максимальне розходження з октавними рівнями російської мови, наведеними в [1], складає 5 дБ.

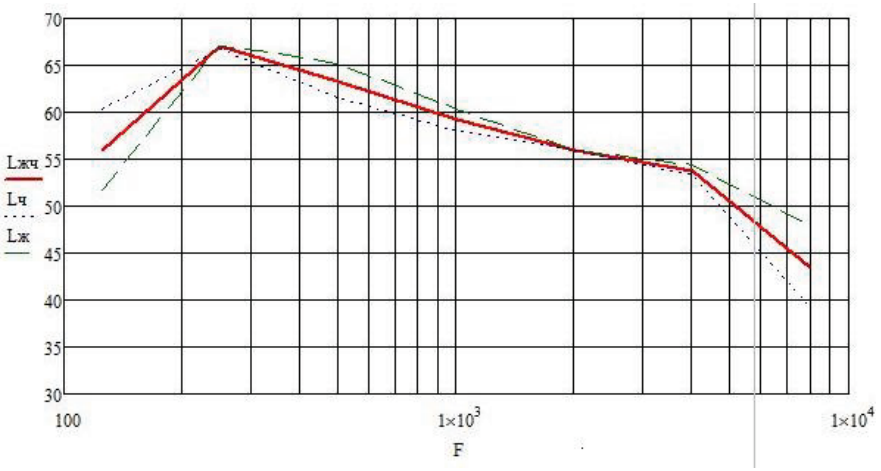


Рисунок 3 – Усереднені для жіночих ($L_ж$) та чоловічих ($L_ч$) голосів і узагальнений ($L_{жч}$) спектри українського мовленнєвого сигналу

В процесі досліджень було виявлено випадки, коли спектри одного й того ж диктора при читанні різних текстів суттєво відрізнялись (рис. 4).

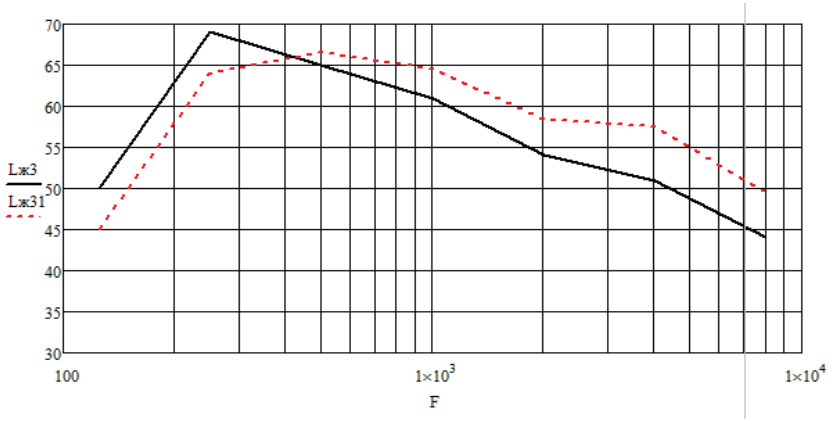


Рисунок 4 – Спектри тривалого мовленнєвого сигналу одного диктора при читанні різних текстів

Це можна пояснити тим, що тексти обирались довільним чином і не враховували статистичні і фонетичні характеристики української мови. Тому доцільним є дослідження впливу підбору текстового матеріалу на спектральні характеристики і уточнення узагальненого спектру тривалих українських мовленнєвих сигналів з використанням фонетично і статистично збалансованого текстового матеріалу, наприклад, артикуляційних таблиць.

Висновки:

1. За аналізом фонограм "живих" дикторських голосів, шляхом визначення октавних рівнів мовленнєвого сигналу, отримано спектр довготривалої української мови, що дає можливість урахувати національні особливості мовлення в оцінюванні захищеності мовної інформації.

2. Необхідно провести уточнення узагальненого спектру українських мовленнєвих сигналів з використанням фонетично і статистично збалансованого текстового матеріалу.

Список літератури:

1. Хорев А.А. (2001) Методы защиты речевой информации и оценки их эффективности. Специальная техника, № 4, С. 22 – 33.

2. Дидковский В.С., Дидковская М.В., Продеус А.Н. (2008) Акустическая экспертиза каналов речевой коммуникации. Монография. Киев, Имэкс-ЛТД, 420 с.

3. Трушин В.А., Иванов А.В., Рева И.Л. (2016) О корректировке методики оценки защищённости речевой информации от утечки по техническим каналам. Специальная техника, № 6, С. 22–30.

4. Касьянов Ю.І., Нужний С.М. (2016) Оцінювання ефективності генератора реальної мовоподібної завади за критерієм розбірливості мови. Вісник Нац. ун-ту "Львівська політехніка": Автоматика вимірювання та керування, №.852, С. 105 – 110.

5. Blintsov, V., Nuzhniy, S., Parkhuts, L., Kasianov, Y. (2018). The objectified procedure and a technology for assessing the state of complex noise speech information protection. Eastern-European Journal Of Enterprise Technologies, 5 (9 (95)), 26–34. doi: http://dx.doi.org/10.15587/1729-4061.2018.144146

6. Покровский Н.Б. (1962) Расчет и измерение разборчивости речи. Москва, Гос. изд-во литературы по вопросам связи и радио, 392 с.

7. Касьянов Ю.І., Трофимчук О.О. (2017) Дослідження спектру довготривалої української мови для оцінювання захищеності мовної інформації формантним методом. Сучасні проблеми інформаційної безпеки на транспорті: Матеріали VII всеукраїнської науково-технічної конференції з міжнародною участю, Миколаїв, НУК, С. 31 – 36.

8. Касьянов Ю.І., Плютенко В.В. (2019) Спектр довготривалої української мови в оцінюванні захищеності мовної інформації за критерієм розбірливості. Інформаційні системи та технології ІСТ-2019: Матеріали 8-ї міжнародної науково-технічної конференції. Харків, ХНУРЕ, С. 243–245.

УДК 004.056.5

ВИЯВЛЕННЯ ЛОКАЛЬНОГО ПОРУШЕННЯ ЦІЛІСНОСТІ ЦИФРОВОГО ЗОБРАЖЕННЯ В УМОВАХ ГЕОМЕТРИЧНИХ ПЕРЕТВОРЕНЬ НЕОРИГІНАЛЬНОЇ ОБЛАСТІ

Автори: *Кобозєва А.А., д.т.н., професор; Бобок І.І., д.т.н., доцент, Державний університет «Одеська політехніка», м. Одеса, Україна*

На сьогоднішній день, враховуючи високий сучасний рівень розвитку інформаційних технологій, проблема виявлення неоригінальних цифрових зображень (ЦЗ) є надзвичайно актуальною. Неоригінальні відеоматеріали можуть привести до непоправних наслідків при їхнім використанні в якості речових доказів у судових розглядах, у медицині, у ході різних маніпуляцій суспільною свідомістю, думкою, у ході політичної боротьби тощо.

На практиці порушення цілісності ЦЗ часто відбувається локально, у межах якоїсь (невеликої) області. Одним з найбільш широко й часто використовуваних програмних інструментів, що приводить до локального порушення цілісності ЦЗ, є клонування, реалізоване у всіх сучасних графічних редакторах. Існуючі методи, що спрямовані на виявлення результатів клонування в ЦЗ, не забезпечують бажану ефективність, зокрема, в умовах додаткової (значної) обробки зображення, в умовах малих розмірів областей клону/прообразу (менше 0.85–1% ЦЗ), в умовах геометричних перетворень клону.

Нещодавно авторами в [1] був запропонований ефективний метод *KL* виявлення результатів клонування, умовою застосовності якого є відсутність відмінностей у постобробці клону й прообразу. Однак на практиці дуже часто клон піддається деяким геометричним перетворенням без зміни безпосередніх значень його елементів та розмірів, що зменшує ймовірність виникнення підозри в наявності клонування з боку зацікавлених осіб.

Метою роботи є забезпечення ефективного виявлення результатів локального порушення цілісності ЦЗ внаслідок застосованого клонування, в тому числі в умовах додаткових збурних дій, зокрема геометричних перетворень клону, незалежно від розмірів клону, шляхом удосконалення методу *KL*.

Основним предметом аналізу в KL є матриця G мінімальних блокових відмінностей (ММБВ), що ставиться у відповідність ЦЗ з $n \times m$-матрицею F (з елементами $f_{ij}, i = \overline{1,n}, j = \overline{1,m}$) за наступним правилом. Нехай $B_{ij}, i = \overline{1,n-l+1}, j = \overline{1,m-l+1}$, – $l \times l$ – блок матриці ЦЗ F, для якого на місці (1,1) знаходиться елемент f_{ij}. Елементи g_{ij} $(n-l+1)\times(m-l+1)$-матриці G відображають величину найменшої відмінності блоку B_{ij} від будь-якого іншого блоку B_{kq} матриці F в сенсі: $\sum_{t,p=1}^{l} r_{tp}$, де $r_{tp}, t, p = \overline{1,l}$, – елементи $l \times l$-матриці R, яка отримана наступним чином:

$$R = \left| B_{ij} - B_{kq} \right|, \tag{1}$$

де права частина рівності (1) розуміється в поелементному сенсі.

Відповідним блокам B_{ij} і B_{kq} клона і прообраза в матриці G відповідають однакові за значенням глобальні (можливо локальні) мінімуми функції, яка інтерполює елементи G:

$$g_{ij} = g_{kq}, \tag{2}$$

що є показником наявності клонування, вказує місця розташування клону і прообразу.

Показано [2], що значення сингулярних чисел квадратної матриці не змінюються при деяких геометричних перетвореннях (відбиття відносно вертикальної та/або горизонтальної осі, поворот на кут, кратний 90 градусам та інші, тобто такі, які не змінюють розміри клону і гістограму значень яскравості його пікселів), що дозволяє використовувати при формуванні ММБВ, яка ставиться у відповідність ЦЗ, для кількісної характеристики відмінності між блоками відмінність їх сингулярних спектрів:

$$g_{ij} = \min_{B_1} \left(round \left(\sum_{i=1}^{l} \left| \sigma_i(B) - \sigma_i(B_1) \right| \right) \right), \tag{3}$$

де функція $round(\cdot)$ округлює аргумент до найближчого цілого значення, $\sigma_i(B), \sigma_i(B_1)$ – СНЧ блоків B, B_1 відповідно, $i = \overline{1,l}$, що є основною ідеєю удосконаленого методу *UKL*. Побудована за запропонованим принципом (3) ММБВ має властивості, аналогічні тим, що були їй притаманні у методі *KL*, зокрема відповідним блокам клону (включаючи випадки його геометричних перетворень) і прообразу відповідають її локальні (глобальні) мінімуми, однакові за значенням (2).

Результати порівняльного аналізу ефективності *UKL* і сучасних аналогів, для чого використовуються два кількісні показники: *TRP* (*true positive rate*) і *FRP* (*false positive rate*):

$$TRP = \frac{\text{кількість ЦЗ, що зазнали клонування, виявлених як клоновані}}{\text{загальна кількість ЦЗ, що зазнали клонування}} \cdot 100\%,$$

$$FRP = \frac{\text{кількість оригінальних ЦЗ, виявлених як такі, що зазнали клонування}}{\text{загальна кількість оригінальних ЦЗ}} \cdot 100\%,$$

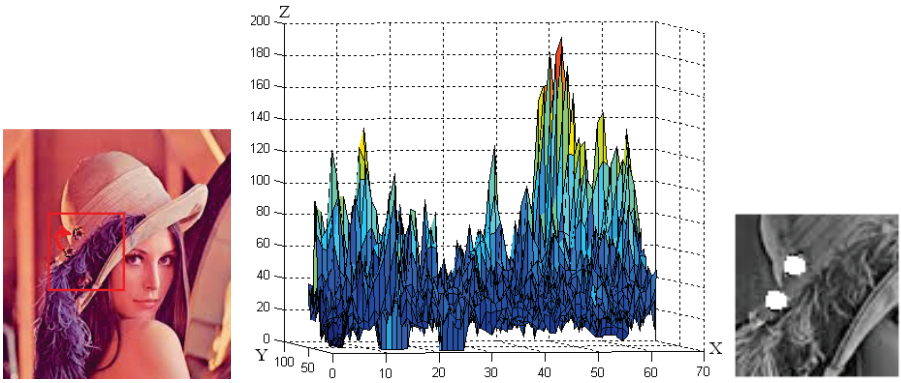
представлені в табл.1.

Ілюстрація роботи *UKL* для конкретного ЦЗ надана на рис.1.

Таблиця 1, рисунок 1 дають наочне представлення про високу ефективність розробленого методу *UKL* виявлення результатів клонування, що є результатом удосконалення *KL*.

Таблиця 1 – Результати порівняльного аналізу ефективності *UKL* і сучасних аналогів

Метод	Pan Xunyu (2010)	Amerini (2011)	Amerini (2013)	Mishra (2013)	Hashmi et al. (2014)	Diaa et al. (2015)	Diaa et al. (2016)	*KL* (2020)	***UKL***
TPR,%	89.96	100	94.9	73.6	80	92	96	100	**100**
FPR,%	1.25	8	9.2	3.6	10	8	2.9	4.8	**5**



а б в

Рис.1. Результат експертизи ЦЗ Lenna методом *UKL* з використанням 8×8-блоків: а – ЦЗ Lenna, яке зазнало клонування з наступним поворотом клону на 90 градусів в від'ємному напрямку; б – графік функції, що інтерполює елементи ММБВ для виділеної частини ЦЗ; в – результат виявлення клону і прообразу

Висновки

В роботі запропоноване удосконалення метода виявлення результатів клонування в цифровому зображенні, що полягає в заміні принципу формування ММБВ (застосуванні сингулярних спектрів блоків матриці зображення), ефективність якого перевищує ефективність сучасних аналогів, залишається значною для клону/прообразу малих розмірів. Удосконалений метод *UKL* забезпечує при тестуванні абсолютне значення показника $TRP = 100\%$, унеможливлюючи пропуск клонованого зображення в умовах наявності геометричних перетворень клону, він є ефективним в умовах мультиклонування, коли одному прообразу відповідає декілька клонів, навіть тоді, коли клони зазнали (різні) геометричні перетворення.

Список літератури:

1. Bobok I.I., Kobozeva A.A., Grygorenko S.M. Method for detecting of clone areas in a digital image under conditions of additional attacks. *Journal of Signal Processing Systems*. 2020. 92. P. 55–69.
2. Бобок І.І., Кобозєва А.А. Теоретичні основи вдосконалення методу виявлення результатів клонування в цифровому зображенні в умовах додаткових збурних дій. *Сучасна спеціальна техніка*. 2018. 1(52). С. 29–39.

УДК 681.3

АЛГОРИТМ МОНІТОРИНГУ ТЕХНІЧНОГО СТАНУ ІНФОРМАЦІЙНО-КОМП'ЮТЕРНИХ МЕРЕЖ НАУКОВИХ УСТАНОВ

Автор: *Козирєв С.С., к.т.н., Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

У зв'язку з ростом інструментальних можливостей наукових експериментальних досліджень лавиноподібно зростає об'єм інформації, яка циркулює в інформаційно-комп'ютерних мережах наукових установ. Необхідність передачі великих обсягів даних, одержуваних в результаті наукових експериментів, забезпечення віддаленого доступу дослідників до унікального наукового устаткування, спільне виконання проектів співробітниками різних наукових лабораторій, організація роботи з базами даних наукової інформації, обмін досвідом та результатами наукових досліджень, різні форми дистанційного навчання, проведення online конференцій в режимі реального часу – все це вимагає наявності гарантоспроможних інформаційно-комп'ютерних локальних мереж науково-дослідних установ.

Науково-дослідні інформаційно-комп'ютерні мережі служать двом основним цілям:

– підтримці роботи дослідників і вчених, шляхом забезпечення їх високопродуктивною інфраструктурою для передачі великих обсягів даних;

– крім того, вони діють як самостійний інструмент дослідника, надаючи віртуальну експериментальну платформу, на якій можна розвинути і перевірити нові технології.

В якості прикладу завдань з наукових досліджень можна розглянути НДР ІІПТ НАН України, основою яких є розробка математичних моделей електрогідроімпульсних процесів з метою подальшого їх використання при розробці розрядноімпульсних технологій для розрахунку оптимальних технологічних режимів, моделювання електророзрядних перехідних процесів при створенні високовольтних імпульсних джерел живлення технологічних систем, розробка алгоритмів і програм для адаптивних систем керування технологічними процесами імпульсного впливу на об'єкти обробки, застосування чисельно-аналітичних методів обробки даних експериментів [1]. Такого типу сучасні дослідження в галузі математичного моделювання та методів обробки результатів експериментальних досліджень тісно пов'язані з новітніми досягненнями в області інформаційних технологій і в основному базуються на обробці великих наборів цифрової інформації.

Наукова інформація, що циркулює в інформаційно-комп'ютерних мережах наукових установ має наукову та комерційну цінність, що викликає необхідність в адекватних та сучасних засобах моніторингу їх технічного стану для забезпечення гарантоспроможності, оскільки збій локальних мереж може паралізувати роботу наукової установи та призвести до відчутних інтелектуальних та матеріальних втрат.

Захист даних у комп'ютерних мережах стає однією з найгостріших проблем. На сьогодні сформульовано три базові принципи інформаційної безпеки: цілісність даних – захист від збоїв, що ведуть до втрати інформації, а також неавторизованого створення або знищення даних; конфіденційність інформації; доступність для всіх авторизованих користувачів [2]. Значну роль в проблемі захисту даних в мережі відіграють апаратні загрози. Модель апаратних загроз комп'ютерної мережі виглядає таким чином: збої кабельної системи; перебої електроживлення; побічні випромінювання збої дискових систем; збої систем архівації даних; збої роботи серверів, робочих станцій, мережевих карт і т. д. [3].

До методів і засобів забезпечення апаратної безпеки відноситься моніторинг функціонування мережі з метою визначення поточного стану та прогнозування. Засоби моніторингу технічного стану ком'ютерних мереж повинні своєчасно виявляти потенційні проблеми об'єктів

мережі, вживати заходи щодо можливої нейтралізації загроз автоматичними засобами або сповіщати системного адміністратора про них.

Кількість об'єктів комп'ютерної мережі наукової установи, які повинні підлягати подібному моніторингу, може бути дуже велика, в залежності від обсягу досліджень. Ось деякі з них: робочі станції; свічі (switches); роутери; сервери; блейд-сервери та ін. Тому важливо вести моніторинг на предмет виявлення технічної несправності або певних тимчасових технічних ускладнень, які мають потенціал стати постійними.

В даній роботі запропоновано алгоритм програми, яка повинна здійснювати перевірку/моніторинг об'єктів комп'ютерної мережі і відповідно або відразу сповіщати системного адміністратора про несправність, або спробувати полагодити її.

Доцільність розробки алгоритму такої програми полягає в тому, що маючи цей алгоритм, можна реалізувати програму засобами будь-якої мови програмування, що використовується відділом системного адміністрування або програмування конкретної наукової установи. Звичайно, існує велика кількість пропрієтарних моніторингових систем, систем з відкритим кодом, безкоштовних та платних, але вони найчастіше занадто складні, бо мають набагато більше функцій, ніж потрібно для задачі технічного моніторингу, а тому потребують значного часу на вивчення документації та встановлення бази даних. Таким чином, написання своєї програми для цілей моніторингу технічного стану стає економічно доцільним вирішенням поставленої задачі.

Блок-схема розробленого алгоритму моніторингу технічного стану наведена на рисунку. Реалізацію програми за таким алгоритмом виконано мовою Perl, яка близька системному адміністратору та нативно сприймаються комп'ютерною операційною системою.

Алгоритм програми зводиться до наступного:

– запуск програми як демона (daemon) для постійного знаходження та отримання інформації;
– визначення категорії об'єкта моніторингу;
– визначення складової частини категорії об'єкта моніторингу;
– виконання заданих тестів/ запитів до об'єкта;
– складання висновку за результатами тестів/запитів;
– аналіз ступеня важливості та критичності несправності, якщо така знайдена;

Рисунок. Блок-схема алгоритму

– спроба усунути несправність програмними засобами автоматично;

– сповіщення персоналу системних адміністраторів про результати перевірки категорії об'єкта моніторингу;

– перевірка наступної категорії;

– після одного циклу перевірки всіх категорій, демон може бути переведений в режим сну (SLEEP) на певний час, а може почати перевіряти знову.

Висновки. Розроблена система моніторингу технічного стану інформаційно-комп'ютерних локальних мереж впроваджена в науковій установі, де показала свою ефективність. В процесі впровадження розглянуто алгоритми роботи тестів аналізу загроз/несправностей та можливі шляхи автоматичної нейтралізації виявлених загроз.

Список літератури:

1. Вовченко, А. И. (2010) Тенденции развития мощных высоковольтных ГИТ в ИИПТ НАН Украины. *Техническая электродинамика*, *№5,* 69-74.

2. Ленков, С. В., Перегудов, Д. А., Хорошко, В.А. (2008) *Методы и средства защиты информации.* Київ: Арий.

3. Козлов, С. Н. (2018) *Защита информации.* Москва: Академический проект.

УДК 004.832.34:004.056.52

ДОСЛІДЖЕННЯ СИСТЕМИ ЗАХИЩЕНОГО ДОКУМЕНТООБІГУ НА БАЗІ ПОРТАЛУ ДЕРЖАВНИХ ПОСЛУГ «ДІЯ»

Автор: *Козирєва Н.Є., магістрант, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна, магістрант, Державний університет «Одеська політехніка», м. Одеса, Україна*

Науковий керівник: *Нужний С.М., к.т.н., доцент, зав. каф. КТІБ, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

Анотація: Дія – український електронний сервіс державних послуг, розроблений Міністерством цифрової трансформації України. Це мобіль-

ний додаток з цифровими документами та портал з публічними послугами.

27 вересня 2019 року Міністерство цифрової трансформації України разом із Fedoriv та Spiilka design büro презентували бренд «Дія».

Платформа Дія — єдина платформа якісних, захищених та об'єднаних державних реєстрів з базами даних. Це крок до сучасного держсервісу в кожному куточку України., крок у цифровізації процесів, який допоможе громадянам отримувати зручні та якісні держпослуги", без зайвих зволікань та черг.

Вступ: Міністерство цифрової трансформації зазначає, що до 2024 року в Україні планується оцифрувати всі державні послуги, охопити 95% населення доступом до якісного інтернету, навчити 6 мільйонів українців базової цифрової грамотності та втричі збільшити обсяг надходжень в IT-галузь.

Додаток та портал «Дія»

16 грудня 2019 року було запущено бета-тест мобільного додатку «Дія», який надавав доступ зі смартфона до цифрового посвідчення водія та свідоцтва про реєстрацію транспортного засобу. Для отримання доступу потрібно було мати і водійські права і техпаспорт, а також необхідно пройти ідентифікацію за допомогою системи BankID у додатках «Приват24» або monobank. Верифікація документів співробітниками поліції відбувалася з допомогою QR-кода.

6 лютого 2020 року відбулася офіційна презентація програми «Дія» за участю вищого керівництва держави. Окрім програми також було представлено онлайн-платформу «Дія. Цифрова грамотність» (укр. Дія. Цифрова грамотність).

Через два місяці після запуску програми його завантажили 2 млн. 25 тис. користувачів.

2 квітня було запущено портал державних послуг "Дія", на якому вже можна було отримати 27 державних послуг онлайн.

У квітні 2020 року у додатку «Дія» також з'явилися цифровий студентський квиток та електронні версії ID-картки та біометричного паспорта для виїзду за кордон.

У травні 2020 року додаток звинуватили у припущенні витоку персональних даних українців, які стали доступними в Telegram. Уряд та

поліція заперечили проти звинувачень на адресу програми, проте джерело витоку даних виявити не вдалося.

2 червня 2020 року додатки оновили налаштування та додали QR-сканер для зручного зчитування та верифікації документів.

5 жовтня 2020 Мінцифри провело презентацію «Diia Summit», на якій представило масштабне оновлення «Дія» («Дія 2.0») – нові електронні послуги в додатку і на порталі. Президент України Володимир Зеленський під час виступу на презентації сказав, що «Україна з наступного року розпочне входження до режиму „paper less", коли державні органи припинять вимагати від громадян паперові довідки чи інші документи для отримання державних послуг».

З 8 по 15 грудня 2020 року Мінцифри проводило Bug Bounty для пошуку вразливих сторін та багів у додатку «Дія». У процесі Bug Bounty було знайдено два технічні баги низького рівня, проте суттєвих недоліків не було виявлено.

Станом на кінець 2020 року 6 млн. українців користувалися додатком, з яких понад 2,6 млн. користувалися оновленою версією. Додаток мав доступ до дев'яти документів і трьох послуг. На порталі «Дія» було вже 50 державних послуг.

30 березня 2021 року Верховною Радою України було ухвалено закон, згідно з яким електронні паспорти в «Дія» зможуть застосовуватися нарівні з паперовими документами починаючи з 23 серпня 2021 року. За словами міністра цифрової трансформації Михайла Федорова, Україна стала першою країною у світі, в якій електронні паспорти мають таку ж юридичну силу, як їхні фізичні аналоги.

1 липня 2021 року в Україні було запущено сертифікати вакцинації від COVID-19, доступні через програму. Є два види сертифікатів – українські, що діють лише всередині країни, та міжнародні, які можна використати за кордоном.

***Мета роботи*:** проаналізувавши наявну інформацію дослідити дослідити слабкі місця в роботі порталу державних послуг Дія.

***Основна частина*:** завантаження платформи Дія на смартфон із App Store або Play Market для безпеки ваших даних, рекомендовано встановлювати лише з офіційних мобільніих перевірених ресурсів.

Після завантаження застосунку користувачу необхідно пройти авторизацію за допомогою BankID. Увійшовши до застосунку користу-

вач зможе вільно користуватися електронними документами, які з'являться у застосунку автоматично, якщо в реєстрах є повні дані.

Зараз у мобільному застосунку доступні такі цифрові документи:

– паспорт громадянина України у вигляді ID-картки;
– біометричний закордонний паспорт;
– картка платника податків (РНОКПП);
– водійське посвідчення;
– свідоцтво про реєстрацію транспортного засобу;
– страховий поліс транспортного засобу;
– студентський квиток;
– довідка переселенця (ВПО);
– свідоцтво про народження вашої дитини.

Цифрові документи мають таку ж юридичну силу, як і пластикові. Це закріплено відповідними нормативними актами.

Вже зараз у застосунку можна отримати наступні послуги:

– оплата штрафів за порушення ПДР;
– оплата боргів за виконавчими провадженнями;
– можливість ділитися копіями цифрових документів;
– перевірка дійсності цифрових документів іншої людини.

Де можна використовувати документи в Дії?

– У випадках, коли потрібно підтвердити свою особу або дійсність документа.
– Під час подорожей.
– Під час отримання поштових відправлень.
– Під час отримання банківських послуг.

Плюси Дія:

– не потрібно бігати різними організаціями, щоб отримати той чи інший документ
– не потрібно йти зайвий раз до лікарні, щоб отримати Ковід-сертифікат
– можна все робити, не виходячи з дому
– документи на руках

– можна забути вдома права
– оплата штрафів на місці

Мінуси Дія:

– страшно, коли твої паспортні (та й не тільки) дані знаходяться на не настільки надійних серверах цієї програми і ними може скористатися хтось ще
– додаток іноді зависає
– у додатку Дія Ковід-сертифікати міжнародного зразка відсутні, є лише внутрішні
– щоб отримати міжнародний сертифікат Ковід, потрібно пройти авторизацію на сайті Дія.
– мало послуг
– не працює, як заявлено
– кількість розчарованих користувачів перевищила кількість задоволених вже на третій день після публікації програми.
– можливість підробити цифровий підпис
– більше чиновників має доступ до тих самих документів, тим вищий ризик витоку і тим менше відповідальності;
– більше даних в об'єднаній системі, тим вища їхня вартість;
– більше доступних послуг, тим вищі ризики зловживань.

Висновок: Після запуску "Дії", в експертному середовищі почали висловлювати побоювання, що дані, які потрапили до мобільного державного додатка, перебувають під загрозою. Були озвучені претензії щодо того, що програмний код не було відкрито для громадськості для аналізу та пошуку помилок. Також було висловлено претензії до ліцензійної угоди.

Довіряти державі небезпечно, вважають в ІнАУ

Додаток державних послуг "Дія" небезпечно використовувати, оскільки має доступ до персональних даних на смартфоні. Так вважає голова комітету Інтернет-асоціації України (ІнАУ) з питань прав людини та свободи слова Максим Тульєв.

Список літератури:

1. Закон України № 4335 «Про внесення змін до Закону України «Про Єдиний державний демографічний реєстр та документи, що під-

тверджують громадянство України, посвідчують особу чи її спеціальний статус».

2. Закон України «Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус»;

3. Постанова Кабінету Міністрів України від 15 квітня 2020 року № 278 “Про реалізацію експериментального проєкту щодо застосування паспорта громадянина України у формі картки в електронному вигляді та паспорта громадянина України для виїзду за кордон в електронному вигляді”;

4. Постанова Кабінету Міністрів України від 28 грудня 2020 року № 1364 «Про реалізацію експериментального проекту щодо реєстрації, зняття з реєстраці місця проживання в електронній формі»

УДК 004.056.5;057.2

РОЗРОБКА СИСТЕМИ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ ЩОДО МЕТОДІВ І ЗАСОБІВ АУДИТУ ІТ-ІНФРАСТРУКТУРИ ПІДПРИЄМСТВА

Автор: *Кравцова О.С., магістрант, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

Науковий керівник: *Турти М.В., к.т.н., доцент, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

ІТ-інфраструктура – це досить складна і неоднорідна система, яка об'єднує всі інформаційні технології та ресурси, що використовуються конкретною організацією або компанією.

Якщо бізнес-процеси організацій і підприємства різних масштабів і форм господарської діяльності повністю інтегровані з ІТ або прагнуть до цього, то саме процеси стають схильні до ризиків кіберсередовища. Для формування умов безперервності бізнес-процесів необхідно проводити роботу по підвищенню рівня інформаційної безпеки (ІБ) інформаційної інфраструктури підприємства (ІТІСП), виявлення

та зниження ризиків, застосовуючи організаційні, програмні та апаратні методи та засоби. На даний час вітчизняними і зарубіжними науковцями розроблено широкий спектр таких методів, засобів та відповідних методик [1-8], однак загальні рекомендації щодо вибору серед них засобів, які є оптимальними для аудиту ІБ конкретного об'єкта інформаційної діяльності, відсутні, що зумовлює актуальність розробки відповідної системи підтримки прийняття рішень. Для вирішення цієї задачі необхідно провести аналіз наявних методів, засобів і методик аудиту.

Метою даної роботи є визначення основних алгоритмів системи підтримки прийняття рішень щодо методів і засобів аудиту ІТ- інфраструктури підприємства (АІТІСП).

Для досягнення поставленої мети необхідно вирішити наступні задачі:

– провести аналіз відкритих літературних джерел і визначити основні етапи АІТІСП;

– визначити вхідні і вихідні дані та склад робіт для кожного етапу АІТІСП.

Комплексний АІТІСП (рис.1) дозволяє отримати найбільш повну і об'єктивну оцінку захищеності інформаційної системи, локалізувати наявні проблеми і розробити ефективну програму побудови захищеної інформаційної системи підприємства.

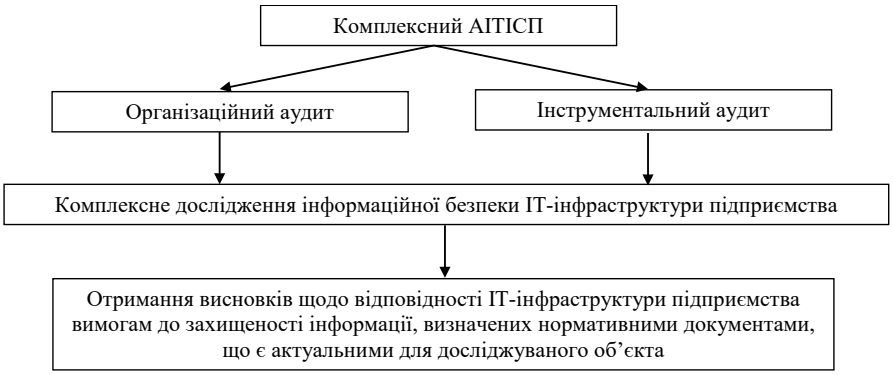


Рисунок 1 – Етапи комплексного АІТІСП

Аудит інформаційної безпеки проводять з метою вирішення наступних завдань:

– перевірка та підвищення рівня захисту інформації до визначених стандартів та вимог;

– планування, розрахунок та оптимізація витрат на забезпечення ІБ;

– обґрунтування інвестицій, що вкладаються в системи захисту інформації, та отримання максимальної віддачі від них;

– підтвердження того, що використовувані внутрішні засоби контролю відповідають завданням організації і дозволяють забезпечити ефективність і безперервність бізнесу.

Проведення АІТІСП замовника здійснюється в чотири етапи:

Етап 1. Постановка задач та уточнення меж виконуваних робіт;

Етап 2. Збирання, систематизація та аналіз наявної інформації;

Етап 3. Проведення аналізу ризиків;

Етап 4. Розробка планів та рекомендацій.

На першому етапі проводяться збирання вихідних даних, їх попередній аналіз, а також організаційні заходи з підготовки проведення аудиту: уточнюються цілі та завдання аудиту; формується робоча група; готується та узгоджується технічне завдання на проведення аудиту.

Метою аудиту може бути як комплексний аудит системи захисту інформації ІТ-інфраструктури підприємства, так і аудит інформаційної безпеки окремих інформаційних систем (мереж передачі даних, обчислювальних систем і систем зберігання даних, та ін.). На цьому етапі уточнюються мета проведення аудиту, а також плануються всі наступні кроки.

До складу робочої групи повинні входити фахівці компанії виконавця (компанії, що проводить аудит) і співробітники компанії замовника. Співробітники замовника забезпечують подання всієї необхідної інформації, контролюють процеси проведення обстеження, а також беруть участь в узгодженні його результатів (проміжних і кінцевих). Фахівці виконавця відповідають за кваліфіковане проведення робіт з обстеження предметних областей відповідно до визначених цілей і завдань проекту.

Етап постановки задач завершується розробкою, погодженням та затвердженням технічного завдання (ТЗ). У ТЗ на аудит фіксується перелік та зміст робіт з аудиту, а також вимоги до розроблюваних до-

кументів. Крім того, в ТЗ вносять строки проведення робіт, а за необхідності – план-графік.

Паралельно з ТЗ розробляється угода про конфіденційність і організовується взаємодія зі службою безпеки замовника.

На другому етапі збирається інформація і дається оцінка наступних заходів і засобів:

- організаційних заходів у галузі інформаційної безпеки;
- програмно-технічних засобів захисту інформації;
- забезпечення фізичної безпеки.

Аналізу та вивченню підлягають наступні характеристики побудови та функціонування ІТІСП:

1. організаційні характеристики;
2. організаційно-технічні характеристики;
3. технічні характеристики, пов'язані з архітектурою ІТІСП;
4. технічні характеристики, пов'язані з конфігурацією мережевих пристроїв і серверів;
5. технічні характеристики, пов'язані з використанням вбудованих механізмів ІБ.

Після отримання вихідних даних готується звіт про обстеження. Звіт про обстеженні є основою для наступних етапів аудиту: аналізу ризиків і розробки планів та рекомендацій.

Проведення третього етапу є важливою стадією при аудиті інформаційної безпеки ІТІСП, оскільки полягає в оцінці реальних загроз порушення ІБ та розробці рекомендацій, виконання яких дозволить мінімізувати ці загрози.

Вихідною інформацією для аналізу ризиків є узгоджений із замовником звіт про проведене обстеження.

Аналіз ризиків дає можливість: оцінити існуючі загрози; ідентифікувати критичні ресурси ІТІСП; виробити адекватні вимоги щодо захисту інформації; сформувати перелік найбільш небезпечних вразливих місць, загроз та потенційних зловмисників; отримати певний рівень гарантій, заснований на об'єктивному експертному висновку.

При аналізі ризиків здійснюється: класифікація інформаційних ресурсів; аналіз загроз; складання моделі потенційного зловмисника; оцінка ризиків порушення інформаційної безпеки.

На четвертому етапі на підставі інформації, отриманої в ході обстеження ІТІСП замовника та результатів аналізу ризиків, розробляються рекомендації щодо вдосконалення системи захисту інформації, застосування яких дозволить мінімізувати ризики, з програмою списку конкретних вразливостей активного мережевого обладнання, серверів, міжмережевих екранів тощо.

По завершенні аудиту готується підсумковий звіт, що містить оцінку поточного рівня безпеки ІТІСП, інформацію про виявлені проблеми, аналіз відповідних ризиків, плани та рекомендації щодо їх усунення.

Результатом АІТІСП є аудиторський звіт, який складається з таких частин, як:

– оцінка поточного рівня захищеності інформаційної системи, а саме: опис та оцінка поточного рівня захищеності інформаційної системи; аналіз налаштувань конфігураційної інформації, знайдені вразливості; аналіз ризиків, пов'язаних з можливістю здійснення внутрішніх і зовнішніх впливів щодо ресурсів інформаційної системи;

– рекомендації щодо технічної складової ІБ: зі зміни налаштувань наявних мережевих пристроїв і серверів; зі зміни конфігурації існуючих засобів захисту; з активації додаткових штатних механізмів безпеки на рівні системного програмного забезпечення; з використання додаткових засобів захисту;

– рекомендації щодо організаційної складової ІБ: з розробки політики інформаційної безпеки; з організації служби ІБ; з розробки організаційно-розпорядчих та нормативно-технічних документів; з перегляду рольових функцій персоналу і зон відповідальності; з розробки програми обізнаності співробітників в частині інформаційної безпеки; з підтримки та підвищення кваліфікації персоналу.

Висновки

В даній роботі проведено аналіз відкритих літературних джерел, визначені основні етапи АІТІСП, а також вхідні і вихідні дані та склад робіт для кожного етапу АІТІСП.

Список літератури:

1. Liebenberg, A., Eloff, JHP MASS: Model for an auditing security system, IFIP Advances in Information and Communication Technology,

Volume 47, 2017, Pages 141-150. URL: https://dl.acm.org/doi/abs/10.1145/3410352.3410761

2. Mukatay G., Bekmanova G., Sharipbay A., Omarbekova A. The audit method of enterprise's Information security / ICEMIS'20: Proceedings of the 6th International Conference on Engineering & MIS 2020. September 2020. Article No.: 29. Pages 1–5.. URL: https://doi.org/10.1145/3410352.3410761
https://dl.acm.org/doi/10.1145/3410352.3410761

3. Sabillon, R., Serra-Ruiz, J., Cavaller, V., Cano, J. A comprehensive cybersecurity audit model to improve cybersecurity assurance: The cybersecurity audit model (CSAM)(Conference Paper), Proceedings – 2017 International Conference on Information Systems and Computer Science, INCISCOS 2017, Volume 2017-November, 29 March 2018, Pages 253--259. URL: https://ieeexplore.ieee.org/document/8328116

4. Кобозєва А.А. Аналіз захищеності інформаційних систем / А.А.Кобозєва, І.О.Мачалін, В.О.Хорошко. – К.: Вид. ДУІКТ, 2010. – 316 с.

5. Кононова, В. О. Оцінка засобів захисту інформаційних ресурсів / В. О. Кононова, О. В. Харкянен, С. В. Грибков // Вісник Національного університету "Львівська політехніка". Комп'ютерні системи та мережі. – 2014. – № 806. – С. 99-104.

6. Овчинніков О.А., Кравцов К.Р. Аналіз методів та засобів захисту ІТ-інфраструктури підприємства //74-а Науково-технічна конференція професорсько-викладацького складу, науковців, аспірантів, та студентів (частина ІІ). – Одеса: Вид-во ОНАЗ ім. О.С. Попова, 2019 – С.124-126.

7. Перун Т. Методологічні засади дослідження механізму забезпечення інформаційної безпеки в Україні Вісник Національного університету «Львівська політехніка». Серія: Юридичні науки. 2017. № 865. С 303-307.

8. Турти, М. В. Розробка блоку прийняття рішень для АСОД ДССЗЗІ / М. В. Турти, С. М. Нужний, А. П. Гунченко // Вісник Національного університету "Львівська політехніка". Автоматика, вимірювання та керування. – 2016. – № 852. – С. 99-105.

УДК 004.056.5:627.25

РОЗРОБКА ШАБЛОНУ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ ДЛЯ ПІДПРИЄМСТВА ПРИПОРТОВОЇ ГАЛУЗІ

Автор: *Нікулін О.С., магістрант, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

Науковий керівник: *Турти М.В., к.т.н., доцент, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

В сучасних умовах Україна перебуває під безперервним інформаційно-психологічним впливом, що обумовлено наявністю політичних, економічних та інших інтересів щодо нашої держави з боку розвинених країн та сусідніх держав, її геополітичним положенням. У цьому контексті проблема забезпечення інформаційної безпеки (ІБ) стосується національних інтересів практично у будь-якій сфері.

Водно-транспортний комплекс України (ВТК) є вагомою складовою економіки держави. Порушення ІБ портів може не тільки спричинити суттєві економічні збитки (наприклад, в разі порушення ІБ таких систем як TOS, що автоматизує операції з вантажами в порту, і CTS, що відстежує рух контейнерів за інформацією з різних каналів передачі даних (найчастіше GPS)), а й негативно вплинути на міжнародний імідж держави. Таким чином, розробка та впровадження цілеспрямованої системної політики захисту інформації від зовнішніх та внутрішніх інформаційних загроз для підприємств припортової галузі (ППГ) є актуальною задачею, розв'язок якої безпосередньо пов'язаний із розробкою та затвердженням процедури створення комплексних систем захисту інформації (КСЗІ). Дослідженню різноманітних аспектів цієї проблеми присвячені праці багатьох науковців [1-3]. При створенні нових портових телекомунікацій на етапах проектування та створення необхідно впроваджувати заходи із захисту інформації за уніфікованими апробованими процедурами, однак, також слід забезпечувати можливість удосконалення КСЗІ в процесі розвитку та удосконалення інфраструктури порту,інформаційно-телекомунікаційних систем (ІТКС), виробничого обладнання, нормативно-правової ба-

зи.Пріоритетними напрямками діяльності, які спрямовані на ефективну реалізацію політики захисту інформації є розробка та затвердження процедури створення КСЗІ в ІТС.

Метою даної роботи єрозробка шаблону КСЗІ для підприємства припортової галузі з врахуванням міжнародного досвіду тагалузевих особливостей забезпечення інформаційної безпеки.

Длядосягненняметибуловизначенонаступнізавдання:

– проаналізувати інформаційну базу дослідження;

– визначити сутність та особливості ІБ портів,як складової безпеки України;

– побудувати шаблон КСЗІ ППГ.

Забезпечення ІБ портів України здійснюється відповідно до:

– Конституції України;

– Морської доктрини України [4], Стратегії розвитку морських портів України на період до 2038 року [5], Стратегії кібербезпеки України і Доктрини інформаційної безпеки України;

– Законів України: «Про національну безпеку України», «Про державну таємницю», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про морські порти України» [6], «Про основні засади забезпечення кібербезпеки України» [7] та ін.;

– Указів Президента України: Про рішення Ради національної безпеки і оборони України від 14травня 2021 року "Про Стратегію кібербезпеки України" [8] та ін.;

– нормативних документів з технічного захисту інформації Державної служби спеціального зв'язку та захисту інформації;

– чинних в Україні міжнародних нормативно-правових актів: Міжнародного кодексу з управління безпекою [9], Міжнародного кодексу з охорони суден та портових засобів [10],Конвенції про кіберзлочинність, ISO 27001 – 27006, ISO 27008, ISO 27010, Керівництва з управління кібер-ризиками у морській галузі (MSC-FAL.1/Circ.3) тощо;

– Постанов Кабінету Міністрів України: Про затвердження Морської доктрини України на період до 2035 року, Деякі питання об'єктів критичної інфраструктури [11] та інше,

– Наказів Міністерства інфраструктури України: Положення про порядок підготовки та подання інформації про вантаж для його безпе-

чного морського перевезення (наказ Мінтрансу України № 497 від 14.12.1998), Правила надання послуг у морських портах України (наказ Міністерства інфраструктури України № 348 від 05.06.2013) тощо.

– та інших нормативно-правових актів, що регулюють відносини в інформаційній сфері і ВТК.

Серед основних завдань державної морської політики Морська доктрина України [4] визначає:

– забезпечення у внутрішніх водах і територіальному морі України та на суднах режимів, що відповідають міжнародному морському праву та міжнародним стандартам безпеки;

– ефективне морське адміністрування.

ВТК відноситься згідно [6] до об'єктів критичної інфраструктури. Рівень критичності може бути оцінений за методикою [11]. Забезпечення ІБ інформації, що циркулює у ВТК сприяє оптимізації функціонування портів і припортових споруд, вирішенню виробничих завдань на суднах в різних режимах функціонування і, як результат, – оптимізації роботи ВТК в цілому.

Сучасні інформаційно-комунікаційні системи ВТКє складними системами, які містять взаємопов'язані компоненти різного ступеня автономності, що обмінюються даними різного змісту і з різними вимогами до захищеності по різним каналам. Комплекс їх засобів захисту таких систем є сукупністю взаємопов'язаних і узгоджених програмних і апаратних засобів, які необхідно обрати із множини наявних на ринку засобів з мінімальними фінансовими витратами, але із гарантованим функціональними можливостями в цілому. При цьому забезпечення достатнього рівня ІБ можливе за умови створення системи управління ІБ відповідно до міжнародного стандарту ISO 27001.

На першому етапі створення КСЗІ формуються загальні вимоги до КСЗІ в ІТКС, яке включає в себе обґрунтування необхідності створення КСЗІ та обстеження середовищ функціонування ІТКС ППГ.

У нашому випадку підставою необхідності створення КСЗІ ППГ є те, що ППГ є підприємством державного сектору, та інформація, яка циркулює в ІТКС ППГ є інформацією з обмеженим доступом та потребує захисту відповідно до чинних законодавчих та нормативних вимог.

Розроблений шаблон містить наступні розділи:

1. Опис інформаційно-телекомунікаційної системи передачі даних.

2. Характеристики інформації, що оброблюється в ІТКС ППГ.

3. Характеристики користувачів ІТКС ППГ.

4. Потенційні загрози інформації, що оброблюється в ІТКС ППГ: модель потенційного порушника, основні типи загроз інформації, що оброблюється в ІТКС ППГ, та способи їх реалізації.

5. Завдання захисту інформації в ІТКС ППГ.

6. Політика безпеки інформації: правила розмежування доступу до інформації, що оброблюється, політика забезпечення доступності інформації та ресурсів, вимоги щодо політики забезпечення спостережності, вимоги щодо політики розподілу обов'язків користувачів.

7. Порядок створення комплексної системи захисту інформації.

ІТКС ППГ являє собою розподілену обчислювальну мережу, до складу якої входять локальні обчислювальні мережі вузла першого рівня та вузлів другого рівня.Всі пристрої захищеної та відкритої серверної зони для забезпечення їх працездатності у випадку аварії електромережі підключені до джерела безперебійного живлення.Стосовно можливостей по доступу до ІТКС ППГ, можна виділити такі категорії користувачів, як користувачі з різними рівнями повноважень і системні адміністратори (першого та другого рівнів), серед яких можна виділити підкатегорії: системні адміністратори програмно-апаратних засобів, адміністратори системи, адміністратори безпеки.

Особливості функціонування ІТКС:

– безперервний цілодобовий режим функціонування серверних компонентів та забезпечення дотримання заявленого часового регламенту оброблення запитів користувачів;

– оброблення як відкритої інформації, так і інформації з обмеженим доступом;

– використання для оброблення інформації прикладного програмного забезпечення, яке створене та підтримуються різними (у тому числі сторонніми) виробниками.

Висновок:

В даній роботі проведено аналіз відкритих літературних джерел, визначені особливості ІБ портів, як складової безпеки України та побудовано шаблон КСЗІ ППГ.

Список літератури:

1. Boyes H., Isbell R., Luck A.CyberSecurityforPortsandPortSystems. – London: InstitutionofEngineeringandTechnology, 2020. – 71 p.

2. Баронова О., Турти М., Мавроді В. Аналіз впливу загроз інформаційній безпеці на проблеми портової галузі // Матеріали 9-ої Міжнародної науково-технічної конференції «Інформаційні системи та технології ІСТ-2020». – Харків: ХНУРЕ, 2020. – С.279-282.

3. Блінцов В.С., Майданюк П.В. Концепція системи захисту інформації, що циркулює на об`єктах морської інфраструктури. Збірник наукових праць НУК. Миколаїв: НУК. 2016. № 1.

4. Про затвердження Морської доктрини України на період до 2035 року: постанова Кабінету Міністрів України від 7 жовтня 2009 р. № 1307. Редакція від 03.11.2020. URL:https://zakon.rada.gov.ua/laws/show/1307-2009-%D0%BF.

5. Про затвердження Стратегії розвитку морських портів України на період до 2038 року: Розпорядження Кабінету Міністрів України від 11 липня 2013 р. № 548-р. Редакція від 23.12.2020. URL: https://zakon.rada.gov.ua/laws/show/548-2013-%D1%80.

6. Про морські порти України: Закон Українивід 17.05.2012. Редакція від 13.02.2020. URL:https://zakon.rada.gov.ua/laws/show/4709-17/ed20200213.

7. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017. Редакція від 01.08.2021. [URL]: https://zakon.rada.gov.ua/laws/show/2163-19.

8. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України": Указ Президента України №447/2021 від 26.08.2021. URL: https://www.president.gov.ua/documents/4472021-40013

9. Міжнародний кодекс з управління безпечною експлуатацією суден та попередженням забруднення (Міжнародний кодекс з управління безпекою (МКУБ)): Резолюція ООН А.741(18) від 04.11.1993. URL:https://zakon.rada.gov.ua/laws/show/995_304.

10. Міжнародний кодекс з охорони суден та портових засобів(Кодекс ОСПЗ) (ISPS) від 12.12.2002. URL:https://zakon.rada.gov.ua/laws/show/896_035.

11. Деякі питання об'єктів критичної інфраструктури: Постанова Кабінету Міністрів України №1109 від 09.10.2020. URL: https://zakon.rada.gov.ua/laws/show/1109-2020-%D0%BF#Text.

УДК 004.056.53: 681.534

НОВІ ПІДХОДИ ДО СТВОРЕННЯ СИСТЕМ ЗАПОБІГАННЯ ВИТОКУ МОВНОЇ ІНФОРМАЦІЇ ЗА МЕЖІ КОНТРОЛЬОВАНОЇ ЗОНИ

Автор: *Нужний С.М., к.т.н., доцент, зав. каф. КТІБ, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

Анотація. В Україні та багатьох інших країнах білий шум або його клони використовуються для активних систем постановки завад в каналах витоку мовної інформації, що дозволяє зловмисникам перехоплювати конфіденційну інформацію. Запропоновано структуру системи захисту мовної інформації на базі генератора завад скремблерного типу. Перехід в системах захисту мовної інформації до такої структури дозволяє відмовитися від застарілого, малоефективного в сучасних умовах, енергетичного зашумлення мовної інформації і перейти до більш продуктивного комплексного методу – енергоінформаційного маскування. Аналіз такого типу завад показує їх високу стійкість до сучасних методів математичної обробки цифрових фонограм, фільтрації завад, реінжинірингу та виділення голосів диктторів. На основі використання методів системного аналізу (абстрагування, експертної оцінки, формалізації та ін.) показано високу ефективність такої системи захисту. Уточнено вимоги до процесу формування основних критеріїв для систем постановки активних завад і їх основних компонентів, а також обмежень у організації і технології їх використання.

Вступ. Мова є найбільш уживаним засобом обміну інформацією. Особливе значення вона набуває при створенні та обговоренні нових та діючих проектів. При цьому, в багатьох випадках, озвучується інформація обмеженого доступу – конфіденційна (конструкторська, економічна, організаційна, know-how та інша), а в певних випадках і таємна інформація. Таким чином, особливого значення набуває її захист.

В роботі розглянуто особливості побудови та функціонування систем захисту мовної інформації (СЗМІ) та запропоновано рішення, яке дозволяє розробляти більш ефективні системи захисту мовної інформації.

1. Мета та задачі дослідження

Метою дослідження є розробка нової концепції створення СЗМІ від витоку акустичними та вібраційними каналами за межі контрольованої зони з урахуванням об'єктивних та суб'єктивних факторів.

Для досягнення мети в роботі були поставлені наступні завдання:

1. Сформувати перелік об'єктивних та суб'єктивних факторів, що впливають на ефективність роботи СЗМІ

2. Запропонувати нові принципи побудови системи постановки активних завад та її вузлів

2. Аналіз факторів, що впливають на ефективність роботи системи захисту мовної інформації

Ефективність роботи СЗМІ залежить від багатьох факторів, які можна розділити на дві групи – об'єктивні та суб'єктивні.

До об'єктивних факторів віднесемо ті, що не залежать від проектувальника і власника СЗМІ. Відповідно, суб'єктивними будуть фактори, які пов'язати тим чи іншим чином з бажаннями, кваліфікацією та можливостями проектувальника і власника СЗМІ.

2.1. Об'єктивні фактори

Проектування та експлуатація СМЗІ у всіх розвинених країнах відбувається в відповідності до нормативного законодавства даної країни, методів, методик та технологій, затверджених відповідними керуючими органами. Відхилення від вимог є суттєвим порушенням і має «жорсткі» реакції та наслідки – тимчасова заборона на роботу об'єкту, заборона на виконання певних функцій, адміністративна та кримінальна відповідальність керівництва об'єкту.

До об'єктивних факторів відносяться:

– Мета та задачі СЗМІ
– Структура СЗМІ
– Тактико-технічні характеристики СЗМІ

2.2. Суб'єктивні фактори

Контроль за працездатністю СЗМІ в виділених приміщеннях (ВП) є задачею спеціально виділеного підрозділу або окремого співробітника. При цьому, в більшості випадків, їх доступ в ці приміщення є суттєво регламентованим, а співробітники, що працюють в ВП не мають відповідної кваліфікації.

Таким чином можна виділити наступні суб'єктивні фактори, які мають суттєвий вплив на працездатність СЗМІ:

– Проектувальники системи:

1. Вибір обладнання, яке встановлюється (безпосередньо тип та марка обладнання, його колір, схема включення та інше).

Аналіз показує, що в більшості випадків є можливість вибору із встановленого переліку обладнання – тобто проявляється певна суб'єктивність проектувальника

2. Кваліфікованість та компетентність проектувальника, які проявляється при оптимізації структури СЗМІ та виконання певних вимог замовника робіт.

Досвіт показує, що при створенні комплексних систем захисту інформації, зазвичай є певний надлишок кількості та можливостей певних елементів обладнання. Замовник може вимагати змінити певні можливості обладнання (наприклад, може вважати, що система акустоконтролю рівня звукового тиску в ВП є засобом підслуховування та інше).

3. Забезпечення паритету між ергономікою ВП і вимогами нормативних документів до СЗМІ.

– Співробітники, що працюють в ВП:

1. Порушення вимог персоналом ВМ організаційних заходів при виконанні технологічного процесу

2. Частина персоналу ВП, зазвичай, має низький рівень знань та компетентностей з інформаційної безпеки:

– Співробітники спеціально виділеного підрозділу (наприклад, відділу захисту інформації – ЗІ) або відповідальний співробітник (група ЗІ):

1. Недостатня кваліфікація співробітників

В відповідності до вимог ДССЗЗІ України [6], кадрове комплектування відділів/груп ЗІ повинно відбуватись виключно спеціалістами, що мають профільну освіту. Однак, в багатьох організаціях та державних установах, посилаючись на недофінансування та відсутність бажаю-

чих, відповідні посади займають співробітники без відповідної фахової освіти.

2. Неналежне виконання співробітниками своїх обов'язків

Аналіз показу, шо в багатьох організаціях та державних установах основним навантаженням співробітників відділів/груп ЗІ є супровід роботи комп'ютерної та оргтехніки, а не проведення заходів по забезпеченню захисту інформації на об'єкті

3. Варіант побудови системи постановки активних завад та її вузлів

Аналіз сучасних методів та технологій виявлення і відновлення мови диктора при значних рівнях шумових завад (як типу білий (гаусовий) шум [3,4,7] та і при використанні завад типу «мовний хор» / «cocktail party» [1,2]) показує їх високу ефективність. Одночасно, це показує низьку ефективність методів та технологій, які є нормативними на даний час, а також недоліки методів визначення рівня захищеності мовної інформації [7–9].

Таким чином, для створення дійсно ефективної системи необхідно використати обмеження, які є в розглянутих метода виявлення, фільтрації завади та відновлення мовного сигналу.

3.1. Альтернатива для білого (гаусового) шуму

Перевагами білого шуму є рівномірність спектральної щільності на всьому діапазоні частот. При цьому самі частоти спектру є випадковими, тобто постійно змінюються. Це стало основною перевагою білого шуму та сприяло його використанню в системах постановки завад.

Однак, при використанні вейвлет- фільтрації [7–9,11], двійкових масок (IBM, IRM) [3,4] та інших методів, заснованих на видаленні випадкових імпульсних сигналів, це і є його головною вадою. Для аналізу використовують віконне перетворення (по октавним смугам) на середньотермінових відрізках часу, співставних з тривалістю фонем/алофонів в людській мові – 0,05…0,25 с.

Таким чином, використання сигналу, який по спектральній щільності був би близьким до білого шуму та створеного на базі модифікованих блоків мови диктора, дає змогу отримати заваду, до якої вказані методи фільтрації є індиферентними.

В загальному вигляді, це є перехід від енергетичного маскування мовного сигналу до інформаційно-енергетичного маскування.

Прикладом такого сигналу маскування є завада «скремблерного» типу, синтез та використання якої розглянуто в [7–10].

3.2. Альтернатива для «мовного хору» / «cocktail party»

Головним принципом, який використовується при синтезі сигналу завади типу «мовний хор» / «cocktail party», є інформаційне маскування. Його принцип заснований на властивостях людського слуху виділяти основного диктора із «мовного хору» при SNR $\geq$ 0 дБ. Якщо співвідношення SNR знаходиться в діапазоні –5 дБ $\leq$ SNR $\leq$ 0 дБ, то відбувається різке погіршення розбірливості мови (сприйняття аудитором мовної інформації). Подальше зменшення SNR призводить до повного маскування мови диктора [12,13].

На практиці розрізняють два типи таких систем [7.8]:

1. «Мовний хор» на основі мови диктора (дикторозалежні системи)
2. Залучення фонограм сторонніх дикторів (дикторонезалежні системи).

Синтез шумової завади за методами «мовний хор» / «cocktail party» створює значні труднощі для зловмисника. На даний час існує декілька методів фільтрації та відновлення мовного повідомлення, втім всі вони потребують значної обчислювальної потужності. Цей показник зазвичай був вирішальним при визначенні можливості доступу зловмисника до інформації, однак поява швидкісного інтернету та майнінгових ферм фактично знівелювало його вагомість.

Вирішенням проблеми є створення для експертної системи конкурентної невизначеності в наслідок наявності великої кількості середньотривалих фонемних блоків створених з мови диктора за деякий попередній проміжок часу.

Такі характеристики має запропонована в [9] система захисту мовної інформації на основі генератора мовоподібного сигналу завади скремблерного типу.

3.3. Особливості побудови системи постановки активних завад та її вузлів

При створенні системи постановки активних завад необхідно врахували наступні чинники:

– Наявність в ВП системи озвучування приміщення

Такі системи встановлюють в кімнатах проведення перемовин, актових залах, тощо. Наявність такої системи дозволяє інтегрувати її з системою постановки активних завад. Структура такої системи представлена в [9].

В разі її відсутності постає задача узгодження структури та місць розміщення її елементів в приміщенні. При цьому набуває значення наступний чинник.

– Психологічний фактор

Постійне акцентування уваги на питаннях кіберзлочинності, а саме на можливості використання мікрофонів та камер смартфонів для шпіонажу за власниками, створили ефект необґрунтованої підозрілості у багатьох людей. Це призводить до неадекватних реакцій на малогабаритні мікрофони в системах захисту мовної інформації (наприклад, в [9] блок контролю рівнів небезпечних сигналів).

Вирішенням цієї проблеми може бути:

1. Використання прихованих мікрофонів, які встановлені безпосередньо в корпусі СЗМІ

2. Використання мікрофону (спікеру), який вбудований в систему внутрішнього зв'язку

3. Використання акустичних і вібраційних вимірювачів небезпечних сигналів на межі ВП (контрольованої зони) [9]

При використанні першого та другого варіантів можливе виникнення інцидентів, пов'язаних з можливістю доступу до таких приладів сторонніх людей. Третій варіант надає більший рівень захищеності, однак має суттєво більшу вартість.

Висновки

На основі використання методів системного аналізу (абстрагування, експертної оцінки, формалізації та ін.) набули подальшого розвитку методи побудови перспективних систем протидії витоку мовної інформації, яка озвучується на об'єктах інформаційної діяльності, акустичними та вібраційними каналами, що дозволило сформувати перелік об'єктивних та суб'єктивних факторів, що впливають на ефективність роботи СЗМІ на основі систем постановки активної завади.

Запропонувати нові принципи побудови системи постановки активних завад та її вузлів шляхом використання в системі постановки активних

акустичних та вібраційних завад генераторів мовоподібного сигналу скремблерного типу, що дає змогу розробляти системи захисту мовної інформації, стійких до її відновлення методами фільтрації та реінжинірингу.

Список літератури:

1. Xianhui, Wang, and Li Xu «Speech perception in noise: Masking anunmasking». Journal of Otology 16 (2021), 109 – 119. Doi:10.1016/j.joto.2020.12.001

2. Jayaganesh Swaminathan, Christine R. Mason, Timothy M. Streeter, Virginia Best, Elin Roverud and Gerald Kidd Jr. «Role of Binaural Temporal Fine Structure and Envelope Cues in Cocktail-Party Listening». Journal of Neuroscience 36 (31) (2016), 8250 – 8257 Doi:10.1523/JNEUROSCI.4421-15.2016

3. Simone Graetzer and Carl Hopkins, «Intelligibility prediction for speech mixed with white Gaussian noise at low signal-to-noise ratios», The Journal of the Acoustical Society of America 149 (2021), 1346 – 1362 Doi:10.1121/10.0003557

4. Graetzer, Simone & Hopkins, Carl. «Comparison of ideal mask-based speech enhancement algorithms for white noise and low mixture signal-to-noise ratios», Proceedings of the 23rd International Congress on Acoustics 9 to 13 September 2019 in Aachen, Germany. Doi: 10.18154/RWTH-CONV-239141

5. Snouden, E. «Lichnoe delo». Moskva: Eksmo, 410. (2020). Available at: https://readli.net/edvard-snouden-lichnoe-delo/

6. Nakaz Administratsiyi Derzhspetszv'yazku vid 19.06.2015 roku № 023

7. Blintsov, V., Nuzhniy, S., Parkhuts, L., Kasianov, Y. «The objectified procedure and a technology for assessing the state of complex noise speech information protection». Eastern-European Journal of Enterprise Technologies, 5 (9 (95)), (2018). 26 – 34. Doi: 10.15587/1729-4061.2018.144146

8. Nuzhnyy, S. M. «Improved technology of evaluation of stage of protection of license information». Modern Information Security, 1 (33), (2018). 66–73. Available at: http://journals.dut.edu.ua/index.php/ dataprotect/article/view/1796

9. Blintsov, V., Nuzhniy, S., Kasianov, Y., Korytskyi, V. «Development of a mathematical model of scrambler-type speech-like interference generator for system of prevent speech information from leaking via acous-

tic and vibration channels». Technology Audit and Production Reserves, 5 (2 (49)), (2019). 19–26. Doi: 10.15587/2312-8372.2019.185133

10. Blintsov, V., Nuzhniy, S., Kasianov, Y., & Korytskyi, V. «Mathematical model of the system of active protection against eavesdropping of speech information on the scrambler generator». Eureka: Physics and Engineering, (3), (2020). 11-22. Doi: 10.21303/2461-4262.2020.001241

11. Renevey, P., Drygajlo, A. «Entropy based voice activity detection in very noisy conditions». In EUROSPEECH – 2001, (2001). 1887–1890. Available at: https://www.isca-speech.org/archive/archive_papers/eurospeech_2001/e01_1887.pdf

12. Brungart D. S. «Informational and energetic masking effects in the perception of two simultaneous talkers». The Journal of the Acoustical Society of America 109 (3), (2001). 1101–1109. Doi:10.1121/1.1345696

13. Brungart, D. S., Simpson, B. D. «The effects of spatial separation in distance on the informational and energetic masking of a nearby speech signal». The Journal of the Acoustical Society of America. 112 (2), (2002). 664-676. Doi: 10.1121/1.1490592

14. Prodeus, A. M., Vityk, A. V., & Didenko, D. Y. Sub'ektivne otsínyuvannya yakostí i rozbírlivostí movnikh signalov, spotvorenikh sintezovanimi shumami. Mikrosistemi, Yelektronika i Akustika, 22 (6), (2017). 56–63. Doi: 10.20535/2523-4455.2017.22.6.101929

15. Zverev V.A. «Slepaya dereverberatsiya rechevogo signala». Akusticheskiy zhurnal, 54, 2, (2008). 307-314. Available at: http://www.akzh.ru/pdf/2008_2_307-314.pdf

16. Wang, Quan; Muckenhirn, Hannah; Wilson, Kevin; Sridhar, Prashant; Wu, Zelin; Hershey, John; Saurous, Rif; Weiss, Ron; Jia, Ye and Moreno, Ignacio. «VoiceFilter: Targeted Voice Separation by Speaker-Conditioned Spectrogram Masking». (2018). Available at: https://arxiv.org/pdf/1810.04826.pdf

УДК 004.056

ДИСПЕТЧЕР ДОСТУПУ ДО ПОТОКОВОГО ВІДЕОРЕСУРСУ

Автор: *Самойленко Д.М., к.ф.-м.н., доцент, завідувач кафедри інформаційних технологій та фундаментальної підготовки, Одеський технологічний університет «ШАГ», м. Одеса, Україна*

Впровадження заходів безпеки у переважній більшості випадків супроводжується встановленням систем відеоспостереження реального часу. З метою оперативного контролю, а також у цілях маркетингу (популяризації послуг в Інтернет) доступ до таких систем здійснюється з декількох моніторів. Нажаль, переважна більшість IP-відеокамер не підтримує великої кількості підключень (не більше 3-5). Це вимагає створення проксі-сервера або розподілювача потоку. Поєднуючи таке завдання з вимогою створення єдиної точки проходження запитів (диспетчера доступу [1]), а також з метою одержання максимального контролю за потоком надаємо перевагу шляху створення власного програмного забезпечення перед встановленням продукції третіх осіб [2].

У роботі пропонується варіант реалізації відображення потокового відео формату MJPEG засобами серверної мови PHP [3]. Основною ідеєю є створення додаткового скрипта (програми), що виконує роль транзитного вузла [4]. У складі клієнтської частини MIP розміщується зображення з періодичним оновленням. Як джерело зазначається транзитний скрипт (img_src.php). Період оновлення визначається налагодженням відеокамери чи мережного обладнання. Наприклад, для потоку у 5 кадрів за секунду, період рівний 200 мс.

```
<img id='cmr' src='img_src.php'><script>function Cadr(){var c=document.getElementById('cmr');
c.src='img_src.php?r=' +Math.random();};
setInterval(Cadr,200);</script>
```

Додавання випадкового числа до запиту забезпечує гарантоване оновлення вмісту контейнера зображення замість використання буферизованих даних. Як можна помітити, у клієнтській частині інформація про реальне розміщення відеокамери відсутня.

Серверна частина системи (img_src.php) має забезпечити комунікацію з відеокамерою. Для цього може бути використано механізм

мережних сокетів. Нехай відео потік доступний за зверненням http://12.34.56.78:910/video.mjpg. Це означає, що він передається з IP адреси 12.34.56.78 через порт 910 за запитом /video.mjpg.

```
$fp = stream_socket_client('12.34.56.78:910');          //відкриваємо сокет-підключення
$out = "GET /video.mjpg HTTP/1.1\r\n";                  //формуємо запит до відео
$out.= "Host: 12.34.56.78:910\r\n\r\n ";                //підтверджуємо розміщення
fwrite($fp, $out);                                      //відправляємо запит
```

У відповідь від камери надходить потік. Оскільки оновлення зображення реалізується клієнтською частиною, серверу достатньо одержати лише один кадр. Для виділення одного кадру з потоку визначаємо його розмір через заголовкову ознаку Content-Length.

```
$l=false;                                               //Ознака розміру кадру
while(($ret = fgets($fp))!= "\r\n")                     //Цикл по заголовках
{ list($h,$v)=split(":",$ret);                          //Розбиття назви і значення
 if(strtolower(trim($h))=='content-length')$l = $v; }   //Пошук потрібного заголовку
```

Для потокових форматів відео цілком можлива ситуація, коли інформація про розмір кадру передається у додаткових заголовках. Тому необхідно додати перевірку і другий пошук за потреби.

```
if($l===false)                                          //Перевірка на відсутність даних
while(($ret = fgets($fp))!= "\r\n")                     //Цикл по додаткових заголовках
{ list($h,$v)=split(":",$ret); if(strtolower(trim($h))=='content-length')$l = $v; }
```

За відомою довжиною кадру здійснюємо його читання з файлового сокет-потоку та передаємо до клієнтської частини MIP:

```
$img=fread($fp,$l);                    //Зчитування кадру
echo $img;                             //Передача даних клієнту
```

Висновки.

У підсумку, система реалізує механізм проксіювання (передачі) відеопотоку від джерела до користувача зі створенням диспетчера доступу. Відокремлення транзитного скрипту, окрім покращення безпеки, відкриває можливість програмного оброблення одержаних зображень, зокрема, для впровадження міток цілісності, часу чи автентичності. Система успішно випробувана на потоках формату MJPEG.

Список літератури:

1. НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. [Текст] / НД ТЗІ, затверджений наказом ДСТСЗІ СБ України від 28.04.1999 № 22.

2. НД ТЗІ 2.5-010-2003 Вимоги до захисту інформації WEB – сторінки від несанкціонованого доступу. [Текст] / НД ТЗІ, затверджений наказом ДСТСЗІ СБ України від 02.04.2003 № 33.

3. Самойленко Д. М. Проектування захищених ресурсів за об'єктно-орієнтованим принципом мовою PHP 5. [Текст] / Самойленко Д. М. // Збірник наукових праць НУК, 2014. – № 3. – с. 83-87 (ISSN 2311-3405)

4. ISO/IEC 7498-1:1994(E) Information technology – Open Systems Interconnection – Basic Reference Model: The Basic Model. [Text] / ISO/IEC 7498-1:1994(E). Second edition. Corrected and reprinted 1996. Switzerland: ISO/IEC Copyright Office. – 68 p.

УДК 004.891.2

МЕТОДИКА СТВОРЕННЯ КОСМПЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ В АВТОМАТИЗОВАНІЙ СИСТЕМІ КЛАСУ 1

Автор: *Смолєнцева О.Ю., магістрант, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

Науковий керівник: *Нужний С.М., к.т.н., доцент, зав. каф. КТІБ, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

Аннотація: Ця стаття складена на підставі нормативно правової базі що наразі існує в Україні щодо інформації та створення її захисту в телекомунікаційних системах. Бурхливе зростання конфіденційної і комерційної інформації, а також істотне збільшення фактів розкрадання інформації викликає підвищений інтерес все більшого числа організацій до створення власних захищених інформаційних систем.

Мова піде про створення комплексну систему захисту інформації на базі АС класу 1, аналіз актуальності, порядок проєктування і створення та розробку переліку організаційної, інформаційної та експлуатаційно-технологічної документації для її створення.

Вступ: Проектування захищених інформаційних систем процес досить складний, який припускає наявність відповідних знань і досвіду, у її творців.

Споживач може не вникати в розробку такого проекту і подробиці його розвитку, проте він зобов'язаний контролювати кожен його етап на предмет відповідності технічним завданням і вимогам нормативних документів. У свою чергу,персональний досвід проектувальників вимагає використання існуючих нормативних документів у цій галузі для отримання найбільш якісного результату.

Таким чином, процес проектування захищених інформаційних систем повинен грунтуватися на знанні і строгому виконанні вимог існуючих нормативних документів, як з боку її розробників, так і з боку замовників.

Існуюча в Україні нормативна база ще не досягла необхідного розвитку в даній області. Так, наприклад, з величезного списку стандартів і нормативних документів України можна виділити лише деякі, які можуть бути використані при проектуванні захищених АС класу 1.

Мета роботи: проведення досліджень та розробка комплекту документів для створення комплексної системи захисту інформації автоматизованої системи на базі класу 1

Основна частина: Відповідно до ст. 28 Закону України «Про інформацію», за режимом доступу інформація поділяється на відкриту інформацію та інформацію з обмеженим доступом.

Відкрита інформація поділяється на інформацію, що належить особі, та інформацію, що належить державі. Інформація з обмеженим доступом в сою чергу поділяється на конфіденційну та таємну (державна таємниця). Конфіденційна інформація може належати особі або державі (інформація, що має гриф обмеження доступу «Для службового користування»).

Відповідно до ст. 8 Закону України «Про захист інформації в інформаційно-телекомунікаційних системах», інформація, яка є власністю держави, або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, повинна оброблятися в системі із застосуванням комплексної системи захисту інформації з підтвердженою відповідністю. Підтвердження відповідності здійснюється за результатами державної експертизи в порядку, встановленому законодавством. Відкрита інформація, що належить державі, потребує захисту в зв'язку з тим, що необхідно забезпечити її цілісність (властивість інформації, яка полягає в тому, що інформація не може бути модифікована неавторизованим користувачем) та доступність (властивість інформації, яка полягає в тому, що користувач, який володіє відповідними повноваженнями, може використовувати інформацію відповідно до правил, встановлених політикою безпеки, не очікуючи довше заданого (малого) проміжку часу, тобто коли ця інформація знаходиться у вигляді, необхідному користувачеві, і в той час, коли вона йому необхідна). Типовим прикладом захисту відкритої інформації може бути захист інформації, розміщеної на офіційному веб-сайті державних організацій – в разі порушення її цілісності деяка інформація на вебсайті може не відповідати дійсності, що скомпрометує діяльність дер-

жавної організації; в разі порушення доступності інформація, що має періодично опубліковуватися на офіційному веб-сайті буде недоступною для ознайомлення користувачів, що порушує їх конституційні права на вільний доступ до інформації.

Комплексна система захисту інформації (КСЗІ) є сукупністю організаційних та інженерних заходів, програмно-апаратних засобів, які забезпечують захист інформації в автоматизованих системах (АС).

До складу організаційних заходів входить складання посадових інструкцій для користувачів і обслуговуючого персоналу, створення правил адміністрування компонент інформаційної системи, обліку, зберігання, розмноження, знищення носіїв інформації, ідентифікації користувачів, розробка планів дій у разі виявлення спроб несанкціонованого доступу до інформаційних ресурсів системи, виходу з ладу засобів захисту, виникнення надзвичайної ситуації.

Інженерні заходи – використання сукупності спеціальних технічних засобів (захищених підключень, міжмережевих екранів, розмежування потоків інформації між сегментами мережі, використання засобів шифрування тощо). Виріб конкретних інженерних заходів та програмно-апаратних засобів залежить від рівня захищеності інформації, який необхідно забезпечити.

За результатами робіт із побудови КСЗІ та Державної експертизи КСЗІ замовник отримує Експертний висновок та Атестат відповідності на КСЗІ, які підтверджують, що побудована КСЗІ коректно функціонує, відповідає вимогам нормативних документів і повністю забезпечує функції захисту, які зазначені в технічному завданні на КСЗІ. Після закінчення терміну дії Атестату відповідності (зазвичай, 5 років) необхідно провести повторну експертизу КСЗІ або створити нову КСЗІ (у випадку якщо існуюча КСЗІ вже не може забезпечити захист від усіх актуальних загроз).

Автоматизовані системи (АС), в яких обробляється інформація, що потребує захисту, умовно поділяється на 3 класи (відповідно до НД ТЗІ 2.5-005):

АС класу «1» – одномашинний однокористувачевий комплекс, що може обробляти інформацію різних категорій конфіденціальності –

тобто це один комп'ютер, який не підключений до локальної мережі або мережі Інтернет;

АС класу «2» – локалізований, багатомашинний багатокористувачевий комплекс, який може обробляти інформацію різних категорій конфіденціальності – наприклад, локальна мережа організації, що не підключена до мережі Інтернет і обробляє відкриту та конфіденційну інформацію.

АС класу «3» розподілений, багатомашинний багатокористувачевий комплекс, який може обробляти інформацію різних категорій конфіденціальності – наприклад, центральний офіс та філії, що передають інформацію через мережу Інтернет.

Мета розробки та створення КСЗІ полягає у виключенні або мінімізації збитку власникові АС та користувачам до припустимого рівня шляхом комплексного використання організаційних (адміністративних) заходів, правових та законодавчих норм, фізичних та технічних (апаратних та програмних) засобів захисту інформації.

Необхідність та обґрунтування створення КСЗІ.

Відповідно до ст.4 Постанови Кабінету Міністрів України №373 від 29.03.2006р., захисту в системі Замовника підлягає:

Відкрита інформація, яка є власністю держави і визначенні Закону України «Про інформацію» належить до статистичної, правової, соціологічної інформації, інформації довідково-енциклопедичного характеру та використовується для забезпечення діяльності державних органів або органів місцевого самоврядування, а також інформація про діяльність зазначених органів, яка оприлюднюється в Інтернет, інших глобальних інформаційних мережах і системах або передається телекомунікаційними мережами;

Конфіденційна інформація, яка є власністю держави або вимога щодо захисту якої встановлена законом, у тому числі конфіденційна інформація про фізичну особу;

Інформація, що становить державну або іншу передбачену законом таємницю.

КСЗІ призначена для забезпечення безпеки критичної інформації та інформаційних ресурсів у процесі функціонування АС.

Мета функціонування КСЗІ полягає в підтримці необхідного рівня інформаційної безпеки АС відповідно політиці безпеки, яка визначається її власником.

Таблиця **Порядок проведення робіт зі створення КСЗІ в АС**

№ п/п	Найменування робіт	Результат робіт	Відповідальний	Узгодження замовника	Узгодження Держ спец зв'язку
Етан № 1. Формування загальних вимог до КСЗІ в АС					
1.1	Обгрунтування необхідності створення КСЗІ	Наказ про створення КСЗІ; Наказ про створення комісії для проведення категорування АС, приміщення; Акт проведення категорування АС, приміщення; Наказ про створення комісії з проведення обстеження АС.	Виконавець Замовник	-	-
1.2	Обстеження середовища функціонування АС	Акт обстеження АС; Перелік об'єктів захисту.	Виконавець	+	-
1.3	Розробка моделі загроз	Модель загроз	Виконавець	+	-
1.4	Формування завдання на створення КСЗІ	Затверджений Акт обстеження та перелік об'єктів і захисту	Виконавець	+	-
Етап 2. Розробка політики безпеки інформації в АС					
2.1	Розробка політики безпеки	Політика безпеки	Виконавець	+	-
Етап № 3. Розробка технічного завдання на створення КСЗІ в АС					
3.1	Розробка технічного завдання	Технічне завдання на створення КСЗІ	Виконавець	+	+
Етап № 4. Розробка технороботочого проекту на створення КСЗІ н АС					
4.1	Розробка технічного проекту	Технічна документація КСЗІ в АС	Виконавець	+	-

№ п/п	Найменування робіт	Результат робіт	Відповідальний	Узгодження замовника	Узгодження Держ спец зв'язку
4.2	Розробка робочого проекту	Робоча документація КСЗІ в АС	Виконавець	+	-
Етап № 5. Впровадження КСЗІ					
5.1	Навчання користувачів АС	Акт завершення навчання користувачів АС	Виконавець Замовник	+	-
5.2	Створення служби захисту інформації	Наказ про створення служби захисту інформації; Положення про службу захисту інформації	Виконавець Замовник	+	-
5.3	Пусконалагоджувальні роботи	Встановлення і налагодження КЗЗ, перевірка і працездатності засобів захисту інформації в автономному режимі та при їх комплексній взаємодії	Виконавець Замовник	-	-
Етап № 6. Попередні випробування КСЗІ в АС					
6.1	Розробка програми та методики попередніх випробувань	Програма та методика попередніх, випробувань	Виконавець	+	-
6.2	Проведення попередніх випробувань	Протокол проведення попередніх випробувань; Акт завершення попередніх випробувань КСЗІ АС	Виконавець Замовник	+	-
Етап №7 Дослідна експлуатація КСЗІ в АС					
7.1	Дослідна експлуатація	Акт приймання КСЗІ в АС у дослідну експлуатацію; Акт завершення дослідної експлуатації КСЗІ в АС	Замовник	+	-
Етап № 8. Державна експертиза КСЗІ в АС					
8.1	Державна експертиза КСЗІ в АС	Атестат відповідності та Експертний висновок	Виконавець Замовник	+	+

Для інформації, що є власністю держави, вимоги щодо її захисту встановлені на законодавчому рівні.

Висновок: Конкретні рекомендації та чітко визначені алгоритми дії для створення комплексної системи захисту інформації в автоматизованій системі на базі класу 1 дають змогу прискорити роботи із її створення, вивченням зайвої нормативно-правової бази та збільшення кількості таких систем.

Список літератури:

1. Закон України «Про інформацію».
2. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах».
3. Концепція технічного захисту інформації в Україні, затверджена постановою Кабінету Міністрів України від 08.10.1997 № 1126 (зі змінами внесеними згідно з Постановою КМ від 07.09.2011 № 938 (938-2011-п)).
4. Положення про технічний захист інформації в Україні, затверджене указом Президента України від 27.09.1999 № 1229.
5. НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.

УДК 681.3

МЕТОДИ І ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ У ТЕХНІЧНИХ КАНАЛАХ НА ПІДПРИЄМСТВАХ

Автор: *Ткаченко О.П., Військова частина 3003 Національної гвардії України, м. Одеса, Україна, магістрант, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

Науковий керівник: *Козирєв С.С., к.т.н., Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

Актуальність даної роботи обумовлена суттєвим збільшенням кількості інформації, зростанням попиту на неї, а отже і зростанням її цінності, у зв’язку з цим зростають і вимоги щодо її захисту. Витік будь-якої інформації може негативним чином відобразитись на діяльності організацій. Особливу роль відіграє інформація з обмеженим

доступом (далі – ІзОД), втрата якої може спричинити негативні наслідки в самій організації та понести за собою матеріальні збитки.

Враховуючи сучасні тенденції до поширення використання портативних джерел обробки інформації, актуальним є захист від витоку каналами побічного електромагнітного випромінювання та наведення (далі – ПЕМВН) саме з таких пристроїв і саме в таких умовах.

Метою роботи є посилення захисту інформації від витоку технічними каналами на підприємствах. Неправомірне перекручування, знищення або розголошення ІзОД може нанести серйозні, а іноді й непоправні матеріальні або моральні втрати. У цьому випадку, досить важливим є забезпечення безпеки інформації з обмеженим доступом.

Для досягнення цієї мети необхідно виконати наступні задачі:

– дослідити наявні технічні канали витоку інформації на підприємствах;

– дослідити джерела витоку інформації по технічних каналах;

– розглянути методи і засоби захисту інформації від витоку технічними каналами.

Однією з найнебезпечніших загроз для інформації, що озвучується на об'єктах інформаційної діяльності або обробляється технічними засобами, в тому числі і інформаційних (автоматизованих), телекомунікаційних, інформаційно-телекомунікаційних систем, є витік інформації технічними каналами.

Під **витоком інформації** розуміється неконтрольоване поширення інформації, яке призводить до її несанкціонованого одержання.

Витік інформації відбувається відповідним каналом витоку. Оскільки засоби розвідки противника, як правило, технічні, то і канали витоку також називають технічними.

ТКВІ – сукупність джерела небезпечного сигналу, середовища поширення небезпечного сигналу та засоби технічної розвідки (далі – ЗТР).

Тобто, ТКВІ є фізичний шлях небезпечного сигналу (носія інформації) від джерела небезпечного сигналу до противника. Також враховуються завади, що діють на вході ЗТР.[1]

Методи захисту інформації на практиці реалізуються із застосуванням засобів захисту. На рис.1 зображено пасивні та активні засоби захисту інформації.

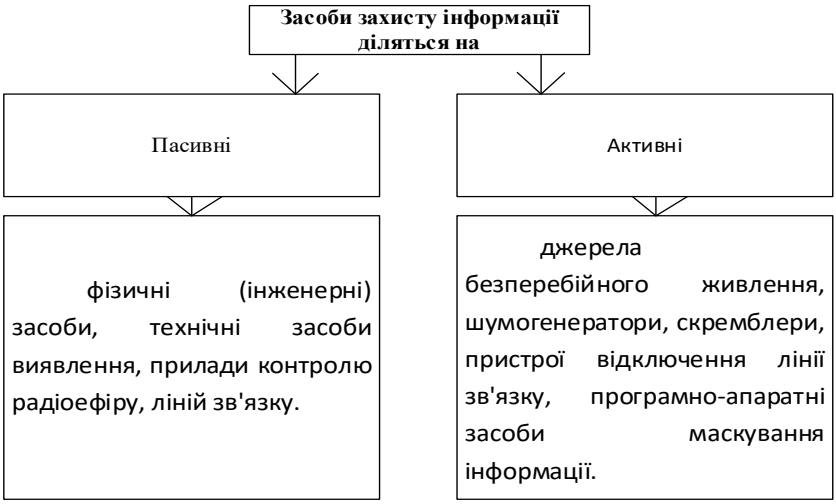


Рис. 1. – Пасивні та активні засоби захисту інформації

Захист інформації від витоку технічними каналами досягається шляхом розробки та реалізації наступних заходів (рис.2):

Рис. 2. – Заходи щодо захисту інформації

Організаційні заходи захисту інформації – це комплекс адміністративних і обмежувальних заходів, спрямованих на оперативне вирішення завдань захисту шляхом регламентації діяльності особового

складу підприємства та порядку функціонування засобів (систем) забезпечення інформаційної діяльності та засобів (систем) забезпечення технічного захисту інформації (далі – ТЗІ).[2]

До основних організаційних і режимним заходів належать:

а) залучення до проведення робіт із захисту інформації організацій, що мають ліцензію на діяльність в галузі технічного захисту інформації;

б) категоріювання та атестація об'єктів інформаційної діяльності (далі – ОІД) і виділених для проведення закритих заходів приміщень (далі виділених приміщень), щодо виконання вимог забезпечення захисту інформації при проведенні робіт з відомостями відповідного обмеженого доступу;

в) використання на об'єктах сертифікованих ОІД і допоміжних технічних засобів і систем (далі – ДТЗіС);

г) встановлення контрольованої зони навколо ОІД та контрольованої території навколо підприємства;

д) залучення до робіт з будівництва, реконструкції ОІД, монтажу апаратури організацій, що мають ліцензію на діяльність в галузі технічного захисту інформації;

е) організація контролю і обмеження доступу на ОІД і в режимних приміщеннях;

ж) введення територіальних, частотних, енергетичних, просторових і часових обмежень в режимах використання технічних засобів, які підлягають захисту;

з) відключення від ліній зв'язку на період закритих заходів технічних засобів, що мають елементи, що виконують роль електроакустичних перетворювачів.

Основні технічні заходи передбачають захист інформації шляхом блокування виявлених загроз із використанням спеціальних засобів ТЗІ.

Усі заходи розробляються одночасно і пов'язуються один з одним.

Організаційні заходи передбачають встановлення:

– окремих завдань захисту ІзОД;
– структури й технології функціонування ТЗІ;
– вимог до забезпечення ТЗІ при організації проектування будівництва (нового будівництва, розширення, реконструкції та капітального ремонту) будівель, споруд і окремих приміщень;
– порядку реалізації організаційних, первинних і основних технічних заходів ТЗІ;

– прав і обов'язків підрозділів і осіб, що беруть участь в обробці ІзОД;

– порядку придбання засобів забезпечення ТЗІ і необхідних нормативних документів;

– контролю й обмежень доступу до виділених приміщень;

– територіальних, частотних, енергетичних, просторових і тимчасових обмежень у режимах використання технічних засобів, що потребують захисту;

– порядку відключення на період проведення закритих заходів технічних засобів, які мають електроакустичні перетворювачі, від ліній зв'язку;

– порядку залучення до проведення робіт із захисту інформації організацій, які мають ліцензію на діяльність у сфері захисту інформації, видану відповідними органами (Держспецзв'язку);

– порядку впровадження захищених засобів обробки інформації, програмних і технічних засобів захисту інформації, а також засобів контролю ТЗІ;

– порядку контролю функціонування СЗІ за її якісними характеристиками;

– порядку проведення атестації СЗІ з розробкою програми атестаційних випробувань. [1]

Висновок

Проведено аналіз розвитку інформаційних технологій, що стимулював розвиток засобів забезпечення безпеки інформації. Розглянуто основні різновиди ТКВІ, основні способи запобігання витоку інформації та унеможливлення створення таких ТКВІ. На основі проведеного аналізу зроблено висновок про необхідність перегляду наявних підходів до вирішення проблем щодо створення СЗІ.

Побудовано модель загроз витоку інформації на підприємствах, що включає наявні технічні канали витоку інформації та джерела витоку інформації по технічних каналах. Запропоновано пасивні та активні засоби захисту інформації з урахуванням особливостей реальних каналів. Розроблено організаційні, технічні та режимні заходи щодо захисту інформації на підприємствах, що оперують інформацією з обмеженим доступом.

Список літератури:

1. Іванченко С.О., Гавриленко О.В., Липський О.А., Шевцов А.С., Технічні канали витоку інформації. Порядок створення комплексів технічного захисту інформації. Навч. Посібник Київ 2016 – 104 с.;
2. Бузов Г.А. Захист від витоку інформації по технічних каналах Навч. посібник / Г.А. Бузов, С. В. Калинин, А.В. Кондратьєв – М: 2005р. – 416 с.

ВІРТУАЛІЗАЦІЯ СИСТЕМИ ВІДЕОСПОСТЕРЕЖЕННЯ

Автор: *Трибулькевич С.Л., старший викладач, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв*

Ідея мережевого відеореєстратора, запущеного на віртуальній машині всередині ПК, лежить на поверхні – таке рішення поєднує плюси виділеного "заліза" (стабільність, висока продуктивність) з дешевизною софтверної системи. Раніше теж можна біло "поселити" пакет для відеоменеджмента в гостьову "операційну", але збірки ОС в реєстраторах спеціально "заточуються" під роботу з відео.

Мережевий відеореєстратор на базі Linux, що працює в середовищах віртуалізації від VMware, Oracle, Xen, Proxmox. А вони, в свою чергу, можуть бути запущені практично на будь-якій платформі: Windows, різних Linux або OS X. В першу чергу, працювати з відео передбачається через веб-інтерфейс.

Не треба вирішувати проблему драйверів – для гостьової системою серед віртуалізації виглядає однаково незалежно від комплектації реального апаратного забезпечення. Найважливіше, що попутно можна виконувати на сервері (або робочої станції) інші завдання. Це не змусить відеореєстратор гальмувати – ресурси для віртуальних машин виділяються жорстко.

Технології віртуалізації дійсно допомагають знизити загальну вартість володіння, і в IT-індустрії цей факт давно визнаний загальновідомим, але архітектори охоронного обладнання підтягнулися тільки зараз.

Система відеоспостереження, яка не перевантажена аналітикою, є більше вимогливою до дискової підсистеми та практично не навантажує процесор відеосерверу. Оскільки процесорні ресурси є вільними їх можна використовувати для інших завдань, саме тут вспливає ідея віртуалізації

відеосерверу. У такій системі можна поєднати переваги декількох платформ відеоспостереження, наприклад, система відеоспостереження Axxon Інтелект має прекрасні можливості запису відеоархіву з камер з високою розподільчою здатністю, але підтримка мобільних клієнтів не відрізнялась високою стабільністю та часто потребувала втручань системних адміністраторів при зміні версії Android або iOS клієнтського пристрою, також керування телеметрією роботизованих камер у платформі Інтелект до недавнього часу потребувало окремої ліцензії на програмне забезпечення. ZoneMinder – вільна система відеоспостереження для ОС Linux, може працювати з практично будь-яким відеопотоком, має підтримку мобільних клієнтів для Android та iOS, розвинутий API інтерфейс для інтеграції у інші систему, яку потребують підключення до відеокамер, наприклад, фотофіксація подій для 1С, дозволяє керувати телеметрією роботизованих камер за допомогою вже готових чи написаних власноруч скриптів, але організація робочого місця оператора системи відеоспостереження не є такою зручною, як у системі Axxon Інтелект. Тому поєднання переваг різних платформ на одному фізичному сервері є актуальною задачею у проектуванні систем відеоспостереження.

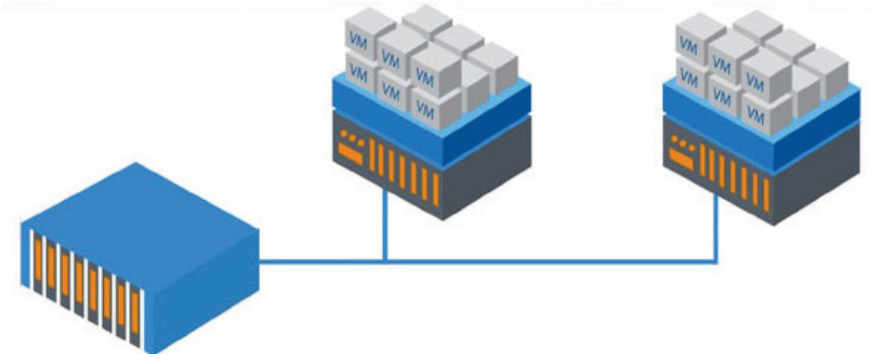


Рисунок 1 – Архітектура ПЗ серверної віртуалізації

Практична реалізація такої задачі можлива лише за рахунок серверної віртуалізації, так як використовуються різні операційні системи

для вказаних вище платформ. Серверна віртуалізація – це архітектура ПО, яке відповідає за те, щоб кілька операційних систем працювали на базі одного фізичного сервера. При цьому ПО кожного сервера самодостатньо й відділене від будь-яких фізичних пристроїв. Це ж ПО сприймає доступні ресурси як ресурси одного фізичного сервера, хоча по факту одержує невеликий пул ресурсів. Віртуальні сервери працюють як імітація фізичного обчислювального обладнання.

У віртуальному сервері емулюється апаратне забезпечення: процесори, дискові накопичувачі, оперативна пам'ять. Операційні системи, установлені на кожний віртуальний сервер, не «бачать» один одного й при цьому функціонують так, ніби вони були встановлені на звичайному комп'ютері. На одному «залозі» можна запускати декілька ОС і в різних пропорціях розподіляти між ними фізичні ресурси.

З віртуалізацією нерозривно зв'язаний гіпервізор – програмне забезпечення, яке розвертається на сервері й прямо взаємодіє з його фізичними ресурсами. Гіпервізор відповідає за те, щоб віртуальні машини «бачили» ці ресурси як власні.

Віртуалізація середовища підвищує гнучкість і адаптивність IT-інфраструктури організації, знижує витрати на її зміст, робить робочі навантаження мобільними, а ресурси – доступними. Наслідками віртуалізації серверів буде ріст автоматизації бізнес-процесів, поліпшення керованості й економічності інфраструктури, мінімізація аварійних і призначених для технічного обслуговування простоїв.

У ситуації із серверами віртуалізація вирішує відразу кілька важливих завдань.

Дозволяє оптимізувати споживання обчислювальних ресурсів і ресурсів зберігання. До появи технології віртуалізації в дата-центрах накопичувалося багато встаткування, яке використовувалося неефективно. Поки одні машини працювали в половину (або менше) свого потенціалу, інші були перевантажені завданнями й часто зупинялися. Віртуалізація розв'язала цю проблему, і тепер робочі навантаження рівномірно розподіляються між декількома машинами.

Стримує ріст кількості серверів. Тепер можна зменшити кількість серверів, необхідних у роботі різним завданням і додаткам, установивши замість них одну машину й запустивши на ній потрібне число ОС (наприклад, сімейства Windows).

Знижує експлуатаційні витрати на зміст фізичного встаткування. Тому що серверів менше, організація може заощадити на енергоспоживанні й кондиціюванні приміщень (знизиться тепловиділення, тому можна буде використовувати менш потужні установки).

Спрощує міграцію даних. При перенесенні даних на інший сервер скорочується час виконання організаційних робіт: IT-фахівцеві досить обновити драйвери на основний (хостовій) ОС, а гостьові продовжать працювати в колишньому режимі, тому що не прив'язані до фізичного встаткування. Для користувачі, які користуються ресурсами віртуальних машин, такий «переїзд» залишиться непоміченим.

Підвищує продуктивність прикладного ПО. Якщо раніше одні додатка на 100 % споживали фізичні ресурси однієї машини, зараз ця ситуація виключена. Працюючі віртуальні машини можуть автоматично переміщатися на менш навантажені сервери, щоб знизити навантаження на більш навантажені.

Робить сервери більш доступними й скорочує простої встаткування. Менше часу потрібно на те, щоб відновити систему до вихідного стану у випадку збою. Віртуальні сервери підтримують технологію створення віртуальних знімків і вміють робити резервне копіювання даних по заздалегідь складеному розкладу.

Спрощує роботу з віртуальним середовищем. Потрібно менше технічних фахівців, які займаються обслуговуванням системи. Адміністратори цінують віртуалізацію за те, що вона дозволяє віддалено управляти віртуальними серверами незалежно від їхньої кількості й територіального розташування. Простий приклад: якщо фізична машина «зависла», більше не потрібно йти в серверну й перезавантажувати її вручну – це можна зробити з консолі зі свого робочого місця.

Citrix Xenserver, Microsoft Hyper-V, Red Hat KVM, ProxMox і Vmware vsphere є найбільшими гравцями на ринку віртуалізації серверів. Найчастіше підприємства зазнають труднощів в ухваленні рішення, який гіпервізор найкраще підійде їхньому бізнесу.

Порівняння кращого програмного забезпечення для віртуалізації серверів на основі функціонала й вимог до встаткування полегшить IT-фахівцям і кінцевим користувачам вибір найбільш підходящого для них гіпервізора.

У рамках задачі цієї статті була досліджена робота системи відеоспостереження ZoneMinder, встановленої на віртуальному сервері під управлінням Debian 10 та розгорнутого у гіпервізорі MicroSoft Hyper-V Server 2016.

Інтерфейс керування гіпервізором представляє собою консоль mmc, яка доступна у операційних системах Windows 8 та вищє. Зовнішній вигляд показано на рис. 2.

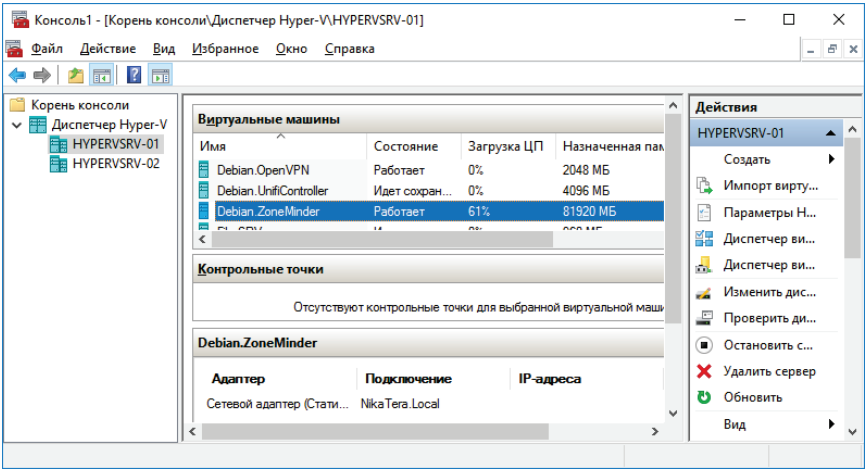


Рисунок 2 – Консоль керування віртуальними машинами Hyper-V

Адміністрування Zoneminder виконується за допомогою будь-якого web браузеру. Сторінка web консолі показана на рис. 3.

Перегляд у реальному часі також можливий за допомогою web браузеру (рис 4), але даний інструмент не є зручним та більш кращим варіантом є використання прикладного клієнтського ПЗ (рис. 5). Керування телеметрією також можливо із клієнтського ПЗ. Недоліком даної платформи є недостатня розвиненість програмного забезпечення для операційних систем Windows: більшість клієнтського ПЗ написана ентузіастами та не сумісна із сучасними версіями Zoneminder або не відповідає відповідним вимогам, підтримка Linux та мобільних клієнтів розвинена достатньо високо і предоставляє широкі можливості для моніторингу.

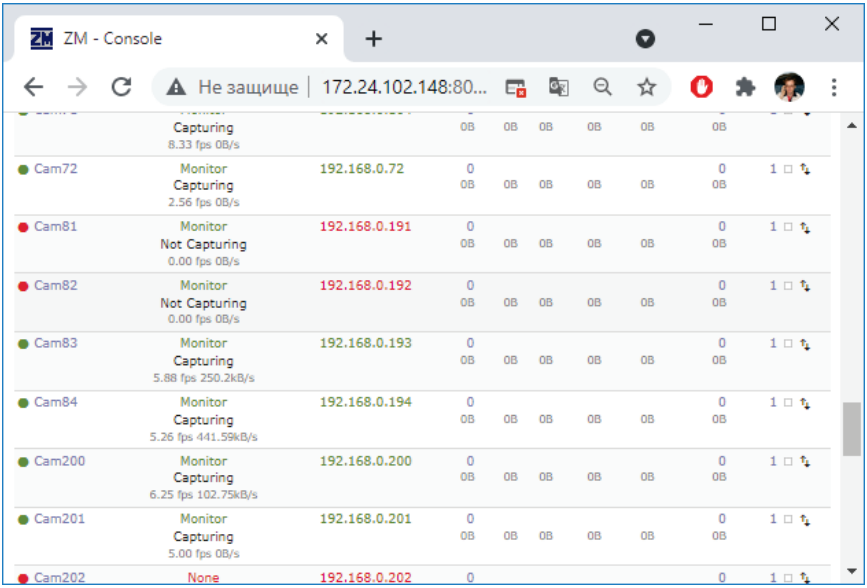


Рисунок 3 – Адміністрування Zoneminder

На сьогоднішній час у рамках комерційної експлуатації у дану систему інтегровано 62 IP камери з розподільчою здатністю від 1920x1080 до 3840x2160, частина IP камер є роботизованими з можливістю керування із клієнтського програмного забезпечення, також на критично важливих ділянках технологічного процесу реалізовано передачу зображення з моніторів операторів у систему відеонагляду із можливістю запису.

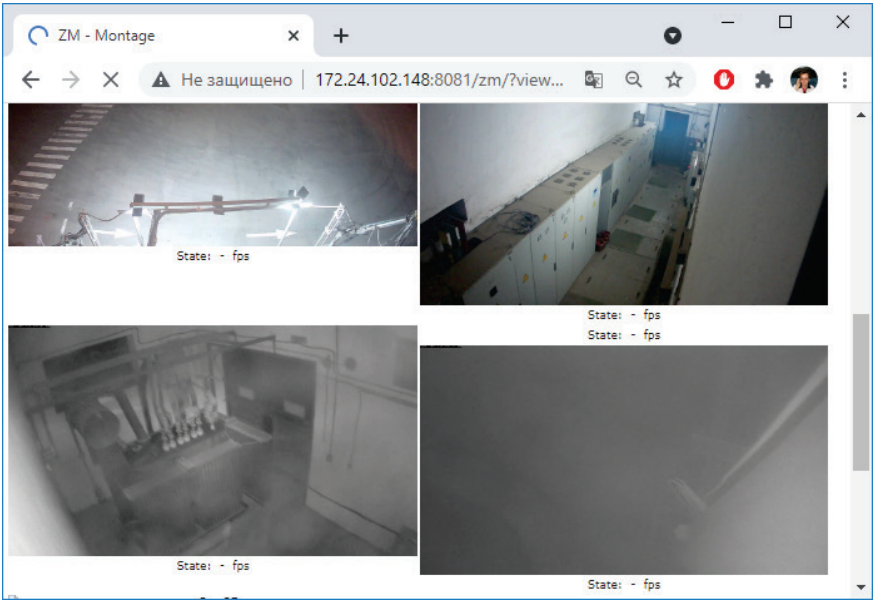


Рисунок 4 – Перегляд у реальному часі

Система Axxon Інтелект (рис. 6) також легко може бути перенесена на віртуальну машину, але для її роботи у системі потрібна наявність апаратних ключів захисту HASP (Hardware Against Software Piracy) – мультіплатформної апаратно-програмної системи захисту програм і даних від незаконного використання та несанкціонованого поширення, розробленої компанією Aladdin Knowledge Systems, згодом придбаною SafeNet. У гіпервізорі Microsoft Hyper-V можливі складнощі для реалізації даної задачі, проте стороннє ПЗ дані функції реалізує без проблем. У інших гіпервізорах, наприклад, Proxmox VE функція передачі USB пристроїв у віртуальні машини працює із «коробки» та не представляє складнощів.

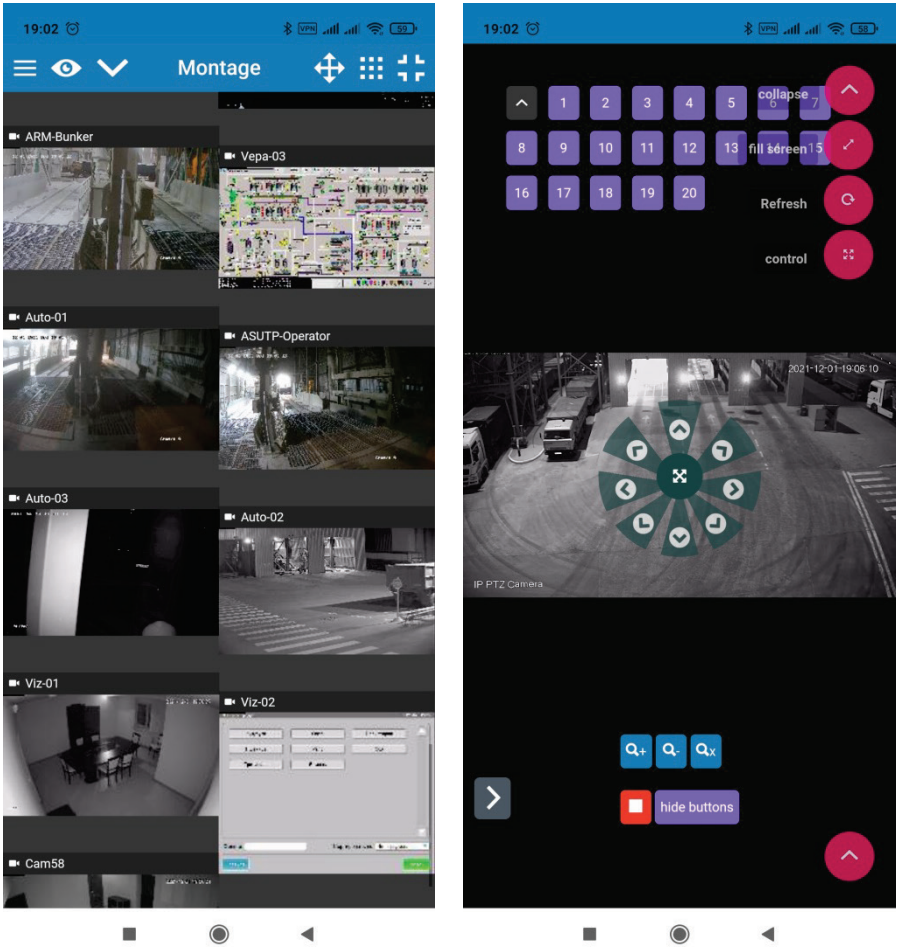


Рисунок 5 – Мобільний клієнт Zoneminder

Рисунок 6 – Система відеонагляду Інтелект

Висновок: Серверна віртуалізація програмної системи відеоспостереження можлива на практично будь-яких гіпервізорах: Microsoft Hyper-V, Red Hat KVM, VMware vSphere та Proxmox VE. До переваг саме віртуалізованої системи слід віднести: централізоване управління, легкість міграції та широкі можливості резервного копіювання за рахунок використання контрольних точок віртуальних машин. Трьохрічний досвід практичної експлуатації даної системи показує її широкі можливості для керування відеонаглядом та оперативного реагування на певні події на об’єкті, також дана система інтегрована за допомогою API із системами обліку.

УДК 004.056.5:627.25

МЕТОДИКИ ВИБОРУ СИСТЕМИ ЗАПОБІГАННЯ ВТОРГНЕННЯМ В КОРПОРАТИВНУ КОМП'ЮТЕРНУ МЕРЕЖУ

Автор: *Холявко О.О., Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

Науковий керівник: *Турти М.В., к.т.н., доцент, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

З розвитком мережевих технологій:

– застосовувані зловмисниками технології стають все більш витонченими;

– програмне забезпечення (ПЗ), використовуване легітимними користувачами, ускладнюється, що призводить до збільшення в ньому кількості помилок і вразливих місць;

– сфера застосування інформаційних технологій постійно розширюється;

– зростають вимоги до мережевої безпеки.

Розробці методів і засобів захисту інформації в локальних мережах присвячені роботи багатьох вітчизняних та зарубіжних науковців науковців [1-8], в тому числі науковців Національного університету кораблебудування [6-8]. Система виявлення вторгнень (англ. Intrusion Detection System, IDS) – необхідна частина сучасних мережевих комплексів захисту. Створення IDS – найбільш перспективна галузь розвитку комп'ютерних технологій. Але поки ці системи недосконалі і містять в собі безліч прихованих проблем, пов'язаних з їх розгортанням, управлінням, масштабуванням і підтримкою.

На даний час існує досить широкий спектр програмних засобів (ПЗ) для виявлення і запобігання вторгнень в корпоративні комп'ютерні мережі (КМ), але методика їх вибору яка враховувала б особливості ПЗ, їх відповідність вимогам користувача і наявним ресурсам, а також особливості програмно-апаратного середовища функціонування, на даний час відсутня.

Метою даної роботи є розробка методики вибору IPS в корпоративну КМ як складової системи підтримки прийняття рішень при формуванні комплексу засобів захисту КМ.

Для досягнення поставленої мети необхідно вирішити наступні задачі:

– провести аналіз засобів захисту мережних ресурсів;
– визначити критерії вибору IPS;
– розробити методику вибору IPS в корпоративну комп'ютерну мережу;

Найпоширенішими прикладами ПЗ захисту інформації в мережі є:

– система контролю і управління доступом;
– антивірусні програми;
– шифрувальне програмне забезпечення;
– мережевий екран;
– сканери вразливостей;
– керування записами;
– Honeypot
– пісочниця;
– система управління інформаційною безпекою
– SIEM (англ. Security information and event management) – програмні продукти, які об'єднують управління інформаційною безпекою SIM (англ. Security information management) та управління подіями безпеки SEM (англ. Security event management). Технологія SIEM забезпечує аналіз в реальному часі подій (тривог) безпеки, отриманих від мережевих пристроїв і додатків. SIEM представлене додатками, приладами або послугами, і використовується також для журналювання даних і генерації звітів в цілях сумісності з іншими даними;
– система виявлення вторгнень (англ. Intrusion Detection System, IDS) – програмний або апаратний засіб, призначений для виявлення фактів несанкціонованого доступу в мережу або несанкціонованого управління ними в основному через Інтернет. Про будь-яку активність шкідливого ПЗ або про порушення типової роботи централізовано збирається інформація SIEM-системою. SIEM-система обробляє дані отримані від багатьох джерел і використовує методи фільтрування тривог для розрізнення несанкціонованої активності від хибного спра-

цювання тривоги. Про що оповіщається або адміністратор або операційний центр безпеки;

– системи запобігання вторгненням (англ. Intrusion Prevention System, IPS) – IDS, які не обмежуються лише оповіщенням, але й здійснюють різні заходи, спрямовані на блокування атаки (наприклад, розрив з'єднання або виконання скрипту, заданого адміністратором). IPS розриває з'єднання і є однім з видів мережевого екрану на рівні додатку. Деякі IPS можуть виявити початок раніше не відомих атак. Системи IPS можна розглядати як розширення IDS, так як завдання відстеження атак залишається однаковим. Однак, вони відрізняються в тому, що IPS повинна відслідковувати активність в реальному часі і швидко реалізовувати дії щодо запобігання атак.

Критеріями вибору IPS обрано:

– призначення IPS (мережеві IPS, IPS для бездротових мереж, аналізатор поведінки мережі, IPS для окремих комп'ютерів);

– бажаний метод реагування на атаку (після початку атаки, блокування з'єднання, блокування записів користувачів, блокування хоста комп'ютерної мережі, блокування атаки за допомогою мережевого екрану, зміна конфігурації комунікаційного обладнання, активне придушення джерела атаки);

– бажаний метод виявлення вторгнень (IPS, які використовують аналіз сигнатур, IPS, які використовують аналіз протоколів; IPS, які використовують виявлення аномалій)

– середовище функціонування;

– вартість;

– вимоги до апаратного забезпечення;

– ефективність.

Ці критерії можуть мати різну вагу, тому для вибору оптимального ріщення за сукупністю критеріїв з врахуванням ваги кожного критерію будемо застосовувати метод аналізу ієрархій

Метод аналізу ієрархій базується на побудові матриць попарних порівнянь і дозволяє визначити відносну важливість в побудованій ієрархії елементів-нащадків для елементів-предків. Матриці попарних порівнянь

будуються для всіх елементів-нащадків, що належать до відповідного предка. Процес побудови матриць попарних порівнянь йде «згори-до низу», тобто спочатку в ролі «предка» виступає мета, а в ролі нащадків – аспекти проблеми і агреговані критерії другого рівня ієрархії. Якщо наявна множина елементів, які є нащадками одного предка, $B = \{B_1, B_2, \ldots, B_n\}$, то їй відповідає множина відповідних ваг елементів або інтенсивностей впливу елементів на предка $W = \{w_1, w_2, \ldots, w_n\}$.

Оптимальну IPS для певної КМ будемо визначати, використовуючи визначену вище систему критеріїв за наступним алгоритмом.

Крок 1. Користувач порівнює групи критеріїв за важливістю. Для цього він заповнює матрицю попарних порівнянь $A = \{a_{ij}\}$ груп критеріїв за шкалою Саатті. Парні порівняння реалізуються в термінах домінування одного елемента-нащадка над іншим у впливі на елемент-предок, для чого використовується бальна шкала, яка може мати різну кількість градацій, в залежності від потреб дослідника системи.

Тобто формування матриці A здійснюється за формулою

$$a_{ij} = \begin{cases} 1 \quad при \quad i = j; \\ \dfrac{1}{a_{ji}} \quad при \quad i \neq j \quad та \quad i > j; \\ \dfrac{a_{1j}}{a_{1i}} \quad при \quad i \neq j \quad та \quad i < j. \end{cases} \tag{1}$$

Крок 2. За матрицею попарних порівнянь груп обчислюються вектори пріоритетів груп за формулою

$$x_i = \frac{\sqrt[n]{\prod_{j=1}^{n} a_{ij}}}{\sum_{i=1}^{n} \sqrt[n]{\prod_{j=1}^{n} a_{ij}}}. \tag{2}$$

Крок 3. Користувач обирає групи критеріїв з найбільшими пріоритетами або всі групи. Якщо якісь групи виключені, то за аналогічно крокам 1 і 2 переобчислюють їх пріоритети.

Крок 4. Для кожної обраної групи *f* визначаються пріоритети підгруп *s* у групі ($P_{pgr}^{f.s}$) аналогічно кроку 1 і 2. Процедуру повторюють до досягнення листя дерева критеріїв $P_k^{f.s.d}$. При цьому *d* – номер критерію в підгрупі.

Крок 5. Визначають пріоритети критеріїв відносно всієї сукупності критеріїв з врахування пріоритетів їх предків

$$P_{Gk}^{f.s.d} = P_{gr}^{f} \cdot P_{pgr}^{f.s} \cdot P_k^{f.s.d}. \qquad (3)$$

Надалі для вибору IPS визначаються матриці попарних порівнянь альтернатив за кожним критерієм, за якими визначаються вектори пріоритетів альтернатив за відповідним критерієм і обчислюється вектор глобальних пріоритетів методів за сукупністю всіх критеріїв з врахуванням важливості самих критеріїв визначаються за формулою

$$PG = \begin{bmatrix} p_1^1 & p_1^2 & \cdots & p_1^r & \cdots & p_1^m \\ p_2^1 & p_2^2 & \cdots & p_2^r & \cdots & p_2^n \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ p_t^1 & p_t^2 & \cdots & p_t^r & \cdots & p_t^m \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ p_n^1 & p_n^2 & \cdots & p_n^r & \cdots & p_n^m \end{bmatrix} \times \begin{bmatrix} pk_1 \\ pk_2 \\ \cdots \\ pk_r \\ \cdots \\ pk_m \end{bmatrix} = \begin{bmatrix} pg_1 \\ pg_2 \\ \cdots \\ pg_t \\ \cdots \\ pg_n \end{bmatrix}. \qquad (4)$$

Оптимальним вибором буде IPS з найвищим пріоритетом.

Висновки:

В даній роботі проведено аналіз засобів захисту мережних ресурсів, визначені критерії і розроблена методика вибору IPS для КМ.

Список літератури:

1. Husák M., Komárková J., Bou-Harb E., Čeleda P. Survey of Attack Projection, Prediction, and Forecastingin Cyber Security // IEEE Communications Surveys&Tutorials. – 2019. – Vol.21. – Issue 1. – PP.640–660.

[URL]: https://www. researchgate.net/publication/327449459_Survey_of_Attack_Projection_Prediction_and_Forecasting_in_Cyber_Security.

2. Бил Дж., Бейкер Э., Казуэлл Б. *Snort* 2.1. Обнаружение вторжений. – Бином-Пресс, 2009. – 656 с.

3. Бурячок В.Л. Технології забезпечення безпеки мережевої інфраструктури. [Підручник] / В.Л. Бурячок, А.О. Аносов, В.В. Семко, В.Ю. Соколов, П.М. Складанний. – К.: КУБГ, 2019. – 218 с.

4. Жук С.Я. Тенденції та перспективи розвитку інформаційної боротьби й інформаційної зброї / С.Я. Жук, В.О. Чмельов, Т.М. Дзюба // Наука і оборона. – 2006. – № 2. – С. 35–41.

5. Зоріна Т.І. Системи виявлення і запобігання атак в комп'ютерних мережах // Вісник Східноукраїнського Нац. ун-ту імені Володимира Даля. -2013 – № 15 (204). – Ч.1 2013. – С.48-52

6. Левченко М.П. Перспективи технології Honeypot, як засобу виявлення та дослідження атак // Матеріали VIII Всеукраїнської науково-технічної конференції з міжнародною участю «Сучасні проблеми інформаційної безпеки на транспорті».-Миколаїв: НУК, 2018 – С.130 – 133.

7. Турти М. Методика оптимізації систем захисту периметра // Матеріали 8-ої Міжнародної науково-технічної конференції «Інформаційні системи та технології ІСТ-2019». 9-14 вересня 2019 р. Харків – Коблеве. – Харків: ХНУРЕ, 2019. – С.254-259.

8. Турти М., Гратій А. Методика вибору спеціалізованого програмного забезпечення для захисту комп'ютерних мереж // Матеріали 9-ої Міжнародної науково-технічної конференції «Інформаційні системи та технології ІСТ-2020». – Харків: ХНУРЕ, 2020. – С.262-266.

УДК 004.056

РОЗРОБКА СИСТЕМИ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ ЩОДО ПРОТИДІЇ ЕЛЕКТРОННІЙ РОЗВІДЦІ

Автори: *Худаніна Н.В., магістрант; Турти М.В., к.т.н., доцент, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

Україна, як і багато інших країн світу, в останні роки зробила сміливі кроки для побудови інформаційного суспільства, забезпечення кібербезпеки та технічного захисту об'єктів критичної інфраструктури.

При цьому Україна набула великий досвід протидії засобам електронної розвідки, у тому числі в ході збройного конфлікту на сході України.

Досвід показує, що особливу роль з точки зору противника в ході отримання закритої інформації відіграє використання засобів оптико-електронної розвідки.

Одна з найважливіших задач, яку доводиться вирішувати фахівцям з технічного захисту інформації – це аналіз наявних властивостей об'єкта захисту, виділення напрямів загроз, визначення критеріїв, що впливають на вибір моделей захисту, вибір кращого варіанта моделі технічного захисту із можливих до застосування.

Прийняти рішення в складних умовах в короткий часовий проміжок для повного і об'єктивного аналізу обстановки дозволяє Система підтримки прийняття рішень.

Розробка структури Системи підтримки прийняття рішень щодо протидії засобам оптико-електронної розвідки є складним завданням. Для досягнення поставленої мети необхідно розв’язати ряд задач:

– проведення аналізу нормативно-правової бази;
– проведення аналізу засобів оптико-електронної розвідки;
– проведення аналізу існуючих систем підтримки прийняття рішень;
– вибір сукупності критеріїв, на основі яких в подальшому будуть оцінюватися і зіставлятися можливі рішення;
– розробка структури Системи підтримки прийняття рішень щодо протидії засобам оптико-електронної розвідки.

Під оптико-електронної розвідкою розуміється процес добування інформації за допомогою засобів, що включають вхідну оптичну систему з оптичним приймачем і електронні схеми обробки електричного сигналу, які забезпечують прийом електромагнітних хвиль видимого та інфрачервоного діапазонів, випроменених або відбитих об'єктами і місцевістю.

Апаратура оптико-електронної розвідки встановлюється на космічних і повітряних носіях, а також може застосовуватися в наземних умовах.

Основними завданнями, які вирішуються при здійсненні захисних заходів від оптико-електронних засобів розвідки (ОЕЗР), є:

– виключення можливості (або зменшення ймовірності) виявлення об'єктів;

– виключення можливості (або зменшення ймовірності) розпізнавання об'єкта;

– виключення можливості (або зменшення ймовірності) визначення параметрів і характеристик об'єкта.

Завдання захисту від ОЕЗР повинні вирішуватися на всіх етапах життєвого циклу об'єкта: проектування, розробка, випробування, виробництво та експлуатація.

До числа основних загальних способів захисту від ОЕЗР відносяться:

– екранування;
– зменшення різниці випромінювання об'єкта і фону;
– зміна параметрів випромінювання та форми об'єкта;
– зміна складу і взаємного розташування об'єктів;
– створення активних перешкод.

З точки зору інформаційної безпеки засоби оптико-електронної розвідки (ОЕР) є одними з найбільш небезпечних, тому мета захисту інформації від несанкціонованого доступу через ОЕР дуже актуальна.

Також варто звернути увагу на те, що прийняття рішення про протидію, потрібних для цього сил і засобів в короткий часовий проміжок вимагає від оператора використання великого обсягу базової інформації, знання нормативних документів, вміння аналізувати інформацію, що надходить. Прийняти рішення в складних умовах дозволяє Система підтримки прийняття рішень.

Система підтримки прийняття рішень (СППР) (англ. Decision Support System, DSS) – це комп'ютерна автоматизована система, метою якої є допомога людям, які приймають рішення в складних умовах для повного та об'єктивного аналізу предметної діяльності.

Система підтримки прийняття рішень вирішує два основних завдання:

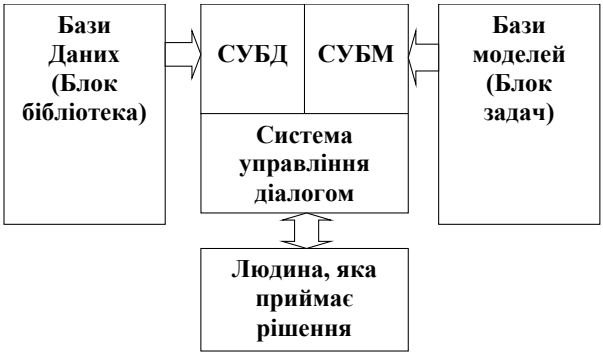
– вибір найкращого рішення з безлічі можливих (оптимізація);
– упорядкування можливих рішень за переважністю (ранжування).

В обох завданнях першим і найбільш принциповим моментом є вибір сукупності критеріїв, на основі яких в подальшому будуть оцінюватися і зіставлятися можливі рішення. Система СППР допомагає користувачеві зробити вибір.

Функціональні СППР є найбільш простими з точки зору архітектури. Відмінною особливістю функціональних СППР є те, що аналізу піддаються дані, що містяться у файлах операційних систем. Перевагами подібних СППР є компактність через використання однієї платформи і оперативність у зв'язку з відсутністю необхідності перевантажувати дані в спеціалізовану систему.

До складу СППР крім оператора входять три головні компоненти:

– підсистема обробки і зберігання даних;
– підсистема зберігання і використання моделей;
– програмна підсистема та блок інтерфейсу. Програмна підсистема включає в себе систему управління базою даних (СУБД), систему управління базою моделей (СУБМ) і систему управління діалогом між користувачем і комп'ютером (СУД).



Бази даних (Блок бібліотека) включає до себе:

– блок засобів ОЕР;
– блок засобів протидії ОЕР;
– блок засобів лазерного випромінювання;
– блок нормативно-правової бази.

Бази моделей (Блок задач) включають до себе:

– модель дослідження засобів ОЕР;
– модель дослідження захисту від ОЕР;

– модель дослідження засобів лазерного випромінювання.

СППР на базі ПЕОМ має функціонувати за наступним алгоритмом:

– моделюється процес зняття інформації засобами ОЕР з лазерного випромінювання;

– аналізуються канали витоку інформації;

– застосовуються заходи протидії засобам ОЕР;

– розраховується ефективність використання саме цих засобів;

– отриманий результат ефективності зіставляється з існуючими нормами захисту;

– формується перелік рішень з різними заходами протидії.

Якщо розрахована ефективність перевищує нормативні параметри, то використаний захисний комплекс є дієвим і користувач може приймати рішення про використання його на практиці з урахуванням специфіки організаційних питань. Якщо ж ефективність є низькою, даний захід не пропонується оператору до переліку рішень.

Список літератури:

1. Бабурин А.В., Пахомова А.С. Физические основы защиты информации // Воронеж – 2015

2. Глушков А.Н., Дробышевский Н.В., Кулешов П.Е Модель оптико-электронного средства как объекта разведки [URL]: https://cyberleninka.ru/article/n/model-optiko-elektronnogo-sredstva-kak-obekta-razvedki/viewer

3. Гуца О.Н., Ельчанинов Д.Б., Порван А.П., Якубовская С.В. Системы поддержки принятия решений в управлении проектами, основанные на качественных методах. [URL]: http://repository.kpi.kharkov.ua/handle/KhPI-Press/28278

4. Крюков С.В., Березовская Е.А. Системы поддержки принятия решений // Ростов на Дону, Таганрог. 2020

5. Куприянов В.В. Компьютерные системы поддержки принятия решений. Учебное пособие. М.: МГГУ, 2010.

6. Майстренко А.В., Майстренко Н.В. Информационные технологии в науке, образовании и инженерной практике // Тамбов – 2009 [URL]: https://www.tstu.ru/book/elib3/mm/2017/maistrenko/t6.html

7. Муромцев Д.Ю., Шамкин В.Н. Методы оптимизации и принятие проектных решений // Тамбов – 2015

8. Оптико-электронная разведка (ОЭР) [URL]: *https://studopedia.su/10_119247_optiko-elektronnaya-razvedka-oer.html*
9. Томашевський В.М. Моделювання систем // Київ – 2005

УДК 004.891.2

УСОВЕРШЕНСТВОВАНИЕ СИСТЕМЫ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ ДЛЯ ОЦЕНКИ УРОВНЯ ЗАЩИТЫ РЕЧЕВОЙ ИНФОРМАЦИИ

Авторы: *Чжан Фучен, магистрант, Национальный университет кораблестроения имени адмирала Макарова, г. Николаев, Украина; Ван Цяньци, магистрант, Государственный университет «Одесская политехника», г. Одесса, Украина*

Научный руководитель: *Нужний С.Н., к.т.н., доцент, зав. каф. КТИБ, Национальный университет кораблестроения имени адмирала Макарова, г. Николаев,Украина*

Аннотация: Эта статья основана на системе оценки распознавания речи искусственной нейронной сети, сочетающей искусственную нейронную сеть и традиционные методы для преодоления недостатков низкой производительности искусственной нейронной сети при описании временных динамических характеристик речевых сигналов и использования преимуществ традиционной речи, распознавание и нейронная сеть. Во-первых, речь предварительно обрабатывается, обнаруживается конечная точка, извлекаются признаки, и, наконец, MATLAB используется при исследовании и проектировании нейросетевой системы, благодаря чему возможности конструктора претерпевают качественные изменения и значительно расширяются.

Введение: В 21 веке, пока традиционные методы оценки качества речи все ещё развиваются, благодаря непрерывному развитию нейронных сетей и технологий глубокого обучения исследователи начали применять нейронные сети для оценки качества речи и продолжают развиваться и улучшаться. Он имитирует отображение восприятия человеческого слуха и использует различные методы машинного обу-

чения для моделирования нелинейного отображения между характеристиками речи и субъективными оценками. Метод искусственной нейронной сети предлагается как новый метод распознавания речи [1]. Это адаптивная нелинейная динамическая система, которая имитирует принцип нейронной активности человека. Этот метод обладает многими превосходными характеристиками, такими как адаптивность, параллелизм, характеристики обучения, отказоустойчивость и надёжность. Этот метод обладает широкими возможностями классификации и улучшенным отображением ввода-вывода способность.

Цель работы: Использование алгоритмов нейронной сети для решения задач оценки речи.

Основная часть: На рис. 1 показана схема предварительной обработки речевых сигналов. В настоящей работе представлены модель распознавания речи на основе искусственных нейронных сетей.

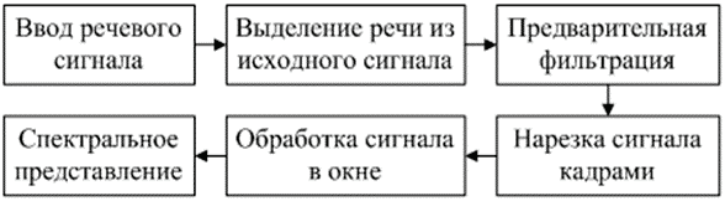


Рис. 1 – Схема предварительной обработки речевых сигналов

Обнаружение конечной точки – ключевой этап в процессе обработки голосового сигнала. В начале голоса неизбежно будет тишина, и тишина повлияет на извлечение голосового сигнала. Тишина может быть устранена путём анализа средней энергии и частоты пересечения нуля речевым сигналом, а, следовательно, и выявлена и сохранена эффективная часть голосовой информации [2].

После того, как речевой сигнал обработан окнами и разделён на кадры, сначала подсчитываются энергия (амплитуда) и частота перехода через ноль каждого кадра, а затем вычисляются статистические характеристики средней энергии и скорости перехода через нуль речевого сигнала. Частота перехода через ноль и энергия получаются в соответствии со статистической характеристикой Threshold. Устанав-

ливаются высокие и низкие пороги для отделения голосовой информации от общего звука.

Только выражая речевой сигнал с параметрами, которые могут выражать его основные характеристики, может быть осуществлено эффективное речевое общение. Скорость синтеза и распознавания речи определяет точность анализа речевого сигнала [3]. Существуют следующие подходы к выделению информативных признаков, описывающих речевой сигнал:

– метод линейного предсказания;
– спектральный анализ.

Спектральный анализ отличается от линейного предсказания тем, что оценки среднего значения усреднённого шума вычитаются из спектра, вычисленного по зашумлённым данным. Наиболее часто употребляются два подхода к классификации и распознаванию:

– мера близости параметров (такая функция называется метрикой);
– нейронные сети.

На рис. 2 показана принципиальная схема структуры нейронной сети.

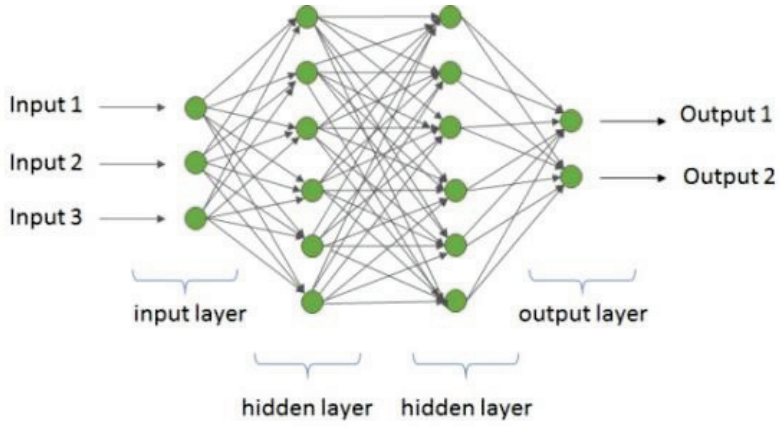


Рис. 2 – Принципиальная схема структуры нейронной сети

Существует два основных способа обучения речевым особенностям в методах нейронных сетей: один – это метод обучения с учителем, а другой – метод обучения без учителя.

Суть метода обучения с учителем состоит в том, чтобы дать результат целевых выходных данных при предоставлении входных данных. Выходные результаты входных данных после обучения функции сравниваются с целевыми выходными результатами, и параметры обучения функции корректируются с помощью этого результата сравнения.

Идея методов обучения без учителя состоит в том, чтобы выводить результаты без целей. Сама система имеет шкалу измерения плюсов и минусов выходных результатов, и параметры настраиваются и оптимизируются в соответствии с этой шкалой измерения.

Вывод. Эта модель нейронной сети имеет только три уровня: входной слой, выходной слой и скрытый слой, поэтому её также называют моделью неглубокой нейронной сети. Структура этой модели проста, но особенность её метода обучения – имитация метода распознавания голоса человеческим мозгом. Модель нейронной сети, использующая алгоритм BP, может обучать правило, основанное на статистической модели из большого количества функций, и предсказывать неизвестные события на основе этого правила. Этот алгоритм также называется многослойным персептроном. Этот алгоритм фактически содержит только скрытый небольшой персептрон в нейронной сети. Однако эта неглубокая модель уже имеет зародышевую форму метода обработки сигналов нейронной сетью человеческого мозга. По сравнению с традиционной технологией распознавания речи, основанной на искусственных технологиях, её эффективность и точность значительно улучшены.

Список литературы:

1. Цай Ляньхун, Хуанг Дэчжи, Цай Руи. Основы и применение современных речевых технологий. Пекин: Издательство Университета Цинхуа, 2003.

2. Тонг Хун. Технические исследования системы распознавания речи по изолированному слову. Цзянсу: Университет Цзянсу, 2009.

3. Ле, Нгуен Виен. Распознавание речи на основе искусственных нейронных сетей / Нгуен Виен Ле, Д. П. Панченко. – Материалы I Междунар. науч. конф. (г. Москва, май 2011 г.). – Москва: Ваш полиграфический партнёр, 2011. – С. 8-11. – URL: https://moluch.ru/conf/tech/archive/3/712/ (дата обращения: 07.11.2021).

СЕКЦІЯ 3. ПРАВОВІ АСПЕКТИ ДІЯЛЬНОСТІ І КАДРОВА ПОЛІТИКА В ГАЛУЗІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

УДК 004.056:623.618

INFLUENCE OF POWER SUPPLIES ON INFORMATION SECURITY AND QUALITY INDICATORS OF AUTOMATED SYSTEMS

Authors: *Li Jiaxian, master; Turty M.V., PhD, Associate Professor, Admiral Makarov National University of Shipbuilding, Mykolaiv, Ukraine*

The share of automated and automatic technological processes in all fields is steadily growing in the modern information society, and accordingly, the role of information protection in the automated systems (AS) of its processing is growing. Often the integrity and / or availability of information is violated due to the loss of power by means of automation of technological processes. Loss of power, in addition, can cause malfunctions of information security hardware, which may also violate the confidentiality of information. On the other hand, the violation of information security can cause failures in the process of information, energy and material exchange in the automated system. Based on this, the development of reliable means to maintain the power supply parameters of the speaker within the technologically determined limits is an urgent task.

The works of many domestic and foreign scientists are devoted to the development of reliable power supply systems (PSS) [1-3]. Such PSSs are governed by complex laws based on many current and projected influencing factors, so their control systems are often artificial intelligence systems [1, 3]. When developing power supply (PS) systems it is necessary to take into account the features of their circuit solutions and features of the operating environment.

The purpose of this work is to determine the characteristics of powerful DC sources (PDCS) and their impact on the information protection of automated systems.

To achieve this goal it is necessary to solve the following tasks: to analyze the circuit solutions of PDCS and determine the parameters that can

affect the security of information; to determine the criteria for assessing the degree of criticality of certain parameters.

PSs can be classified according to various criteria, in particular, by type of current and power. By type of current power sources are divided into DC sources and AC sources. Alternating current sources can be further classified by the number of phases. According to power, PSs are divided into very low, low, medium and high power sources. According to the type of output, there are current sources, voltage sources and power sources. PDCSs are designed to provide electrical equipment with a power that is provided by technical requirements and safety. Such devices provide a constant voltage, regulating its strength and stability. Most electronic circuits require a DC power supply.

According to the principles of conversion of energy sources, PDCSs are divided into the conversion of AC energy into DC energy and sources with conversion into DC energy of other types of energy (solar energy, thermal energy, chemical energy, mechanical energy). The transducers used in PDCS can be uncontrolled controlled. In the latter cases, PDCS circuits have a control system that generates control signals. Input and output control systems can be used as information signals. These signals are transmitted through their own channels and can be affected by interference in these channels. Interference in the transmission channels of the control signals can be caused both by random factors and by violation of the electronic compatibility of the power part of the conversion unit and the control system. This is more dangerous for powerful power sources, which leads to a violation of the rated mode of equipment that consumes a lot of power is dangerous. The block diagram of a DC PS with a controlled rectifier is shown in Fig.1.

When designing automated systems in accordance with the IEC 60364 standard, it is necessary to know the characteristics of the power supply: type of electric current (alternating and/or constant); types of conductors created in electrical conductors of electrical installations (for direct current: pole (pole) conductor, middle conductor, protective conductor); allowable voltage values and allowable voltage deviations; frequency and permissible frequency deviations; maximum allowable current; expected short-circuit currents; full ground circuit before entering the electrical installation; voltage losses,

voltage fluctuations and voltage drops; type and nominal characteristics of the device of protection against overcurrents established on electric installations (protection in the electric circuit of a direct current can be by means of use of grounding of the middle part which is under pressure).

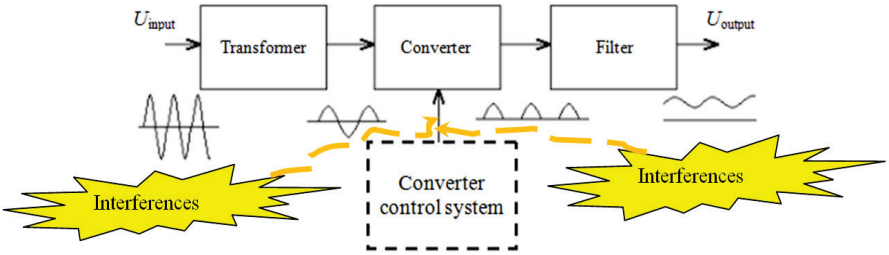


Figure 1 – Block diagram of PDCSs

The quality of electricity is compared with the established quality standards. There are two types of quality standards: normally permissible and maximum permissible standards.

The operation of the AS may be affected by the following power failures: voltage deviation is a change in the amplitude (current) value of the voltage; the amount of voltage is this (with a certain frequency) or repeated at free intervals change the amplitude value of the voltage; voltage failure is a decrease in voltage below 90% of the rated voltage with subsequent recovery of the voltage to the original or approximately to this value; temporary overvoltage is an increase in voltage by more than 10% of the rated voltage; voltage pulse is a sharp short-term change of voltage with the subsequent restoration of voltage to the initial or approximately to it value; non-sinusoidal voltage is the deviation of the shape of the voltage curve from the ideal sinusoid which is characterized by the coefficient of curvature of the sinusoidal shape of the voltage curve and the coefficients of the harmonic components of the voltage; frequency deviation is the difference between the frequency of alternating current and the nominal value; low-frequency perturbations – are failed and there are voltages that are comparable to the voltage period of the power supply, and which are included in

the voltage spectrum of low-frequency and high-frequency harmonics; high-frequency perturbation pulses, which are superimposed on the sinusoidal voltage of the primary network and distort the shape, are included in the voltage spectrum of the high-frequency harmonic; instantaneous loss of power supply in case of accidents; delayed power loss in accidents.

Different types of machines (as power consumers) have different requirements for PSSs [4]. PDCS are used in various fields [5]: mechanical DC power supply is used in thermal power plant, hydroelectric power plant, etc. (turbine generator and hydroelectric generator); chemical power supply has been widely used in production economy, science and technology, military and daily life (dry cell, battery, etc); heat energy is used in satellites, space probes and unattended remote facilities(equipment radioisotope thermoelectric generators; solar energy is used in solar power field, aerospace, etc. (solar panels).

DC is commonly found in many extra-low voltage applications and some low-voltage applications, especially where these are powered by batteries or solar power systems.

Most electronic circuits require a DC power supply. High-voltage direct current electric power transmission systems use DC for the bulk transmission of electrical power, in contrast with the more common alternating current systems. For long-distance transmission, such systems may be less expensive and suffer lower electrical losses.

Telephone exchange communication equipment uses standard 48 V DC power supply. Other devices may be powered from this PS using a DC-DC converter to provide any convenient voltage.

Most automotive applications use DC. An automotive battery provides power for engine starting, lighting, and ignition system. Most highway passenger vehicles use nominally 12 V systems. Many heavy trucks, farm equipment, or earth moving equipment with Diesel engines use 24 V systems. There are automotive applications that use 6 V and 42 V systems too.

Light aircraft electrical systems are typically 12 V or 24 V DC similar to automobiles.

Other fields, where PDCSs are traditional awidely studied and applied, are electroplating, welding machine, electric vehicle charging, metal pipeline cathodic protection.

In the field of aerospace, aerospace communication system has the characteristics of specificity and confidentiality, especially high timeliness requirements. The reliability of communication power supply is the primary consideration of aerospace communication as an important guarantee for the safe operation of communication systems. 240V high voltage DC power supply system (HVDC), as a simple and reliable technology, reduces the power conversion process, improves the reliability and efficiency of power supply[5].

Thus, at present, the UPS system is widely used as the main power supply of IT equipment in automated systems with various functional enviroment to overcoming the system interruption caused by the interruption of electricity supply. However, such systems accidents often occur due to UPS itself or even the faults of parallel redundant systems, which can caused great social impact and considerable economic losses: overloading of power supplies of electronic devices, reducing their life; shutdown of equipment at insufficient voltage for its operation; failure of electric motors; data loss in computers; failures in the execution of programs and data transmission; unstable image on monitor screens and video systems.

The type of uncontrolled rectifier used in the power supply determines: form of output voltage; coefficient of pulsations at the output; the average value of the voltage on the DC side; load of phases on the side of alternating current; dependence of quality indicators on the nature of the load. If the rectifier is controlled, the control law significantly affects all indicators.

The influence of random factors or deliberate actions of attackers can distort control signals. Even simple rectangular control signals that are delayed or have too large an amplitude (the magnitude of the control signal is dangerous for the controlled device) or too small an amplitude (the magnitude of the control signal is insufficient to operate the controlled device) significantly affect the output voltage and average voltage in side of direct current, and can also cause high-frequency perturbations at the output, decrease and increase of voltage, voltage dips, etc.

With the increasing requirements for high-power DC power supply in aviation, military and chemical fields, the importance of parallel power supply technology is increasing due to the dual limitations of power electronic

devices and transformer power capacity, so current-sharing technology becomes the key to realize high-power DC power supply [6]. Modern PDCSs are complex systems. For example, the Liaoning University of Technology has developed a High Power DC PS based on Network Monitoring [7]. Based on the current situation of DC PS equipment operation, monitoring and maintenance, a management mode of DS PSS network management and status check and repair of substation is put forward and implemented. Computer technology, measurement and control technology, optical fiber network communication technology, intelligent fuzzy neural network technology is applied to the substation dc power supply system, the scattered around in DC charging machine operation parameters, battery operation parameters, system running state through the optical network transmission to the central server, carries on the real time monitoring, analysis and fault diagnosis, The equipment maintenance from planned maintenance to state maintenance transition, not only to ensure the safe and reliable operation of electrical equipment, but also to obtain economic and social benefits [6].

In systems of this type, the violation of information security in the channels of transmission of control signals will have even more significant consequences.

Conclusions

When designing power supplies, the choice of circuit solutions should be based not only on the properties of the rectifier circuit, but on the results of assessing the stability of the output parameters of the power supply in case of electromagnetic compatibility and information security. The severity of the distortions of the control system signals depends on the field of application of the automated system, type of load, requirements for the impact on the AC power supply, rectifier circuit, degree of amplitude distortion, shape and time characteristics of control signals. Thus, in this work the circuit solutions of PDCS have been analyzed; the parameters of PDCS that can affect the security of information and the criteria for assessing the degree of criticality this criteria have been determined.

References:

1. AragüésPeñalbaM., NguyenT.L., CaireR., SumperA., GalceranArellanoS.,Tran-Quoc T. General form of consensus optimization for distributed OPF in HVAC-VSC-HVDC systems // International Journal of

Electrical Power & Energy. – Vol.121, – 2020. URL: https://www.sciencedirect.com/science/article/abs/pii/S0142061519337639.

2. Villafáfila R., Sumper A., Montesinos-Miracle D., Sudrià-Andreu A., Jaureguialzo, D. E.J. Selection criteria of high-power static Uninterruptible Power Supplies //Electrical Power Quality and Utilisation: 9th International conference: EPQU 2007. – Barcelona, 2007, P. 1-5. doi: 10.1109/EPQU.2007.4424196. URL: https://ieeexplore.ieee.org/ document/4424196.

3. Турти М. Вибір джерел безперебійного живлення автоматизованих систем з врахуванням вимог інформаційної безпеки // Матеріали 9-ої Міжнародної науково-технічної конференції «Інформаційні системи та технології ICT-2020». – Харків: ХНУРЕ, 2020. – С.250-257.

4. Eckoldt H.-J. Different power supplies for different machines // CERN Accelerator School, CERN-2006-010. – P.385-404 URL: https://cds.cern.ch/record/987563/files/p385.pdf.

5. Dongliang L. Application of 240V high voltage DC power in space communication system // Electric Technology. – 2017. – №(12). – P.4. URL:http://dqjs.cesmedia.cn/CN/Y2017/V18/I12/142

6. Hong W., Guanghui Z., Zhiqiang L., et al. Network Management and Maintenance of DC power System // Power Grid Technology. – 2010. – №034(002). – PP.185-189. URL: https://kns.cnki.net/kcms/detail/ detail.aspx?dbcode=CJFD&dbname=CJFD2010&filename=DWJS201002037&uniplatform=NZKPT&v=y1sGBwWN2ujq7faJWddNcnXxjQaoPe3m0sCX1OkF_iOKRFOvsqElyNXhMDHP7MO

7. Yingying W., Lie Z. Research on parallel current sharing technology of high-power DC power supplies//ModernComputer.2018.№(19).P16-19. URL: https://kns.cnki.net/kcms/detail/detail.aspx?dbcode=CJFD&dbname=CJFDLAST2018&filename=XDJS201828005&uniplatform=NZKPT&v=lNMk_PvKfz3qOww7y9Ectv2QYhnbPcRt8stugEk19q25Z95WZNZnGzAj_OUedNk

УДК 004.056.5;057.2

DEVELOPMENT OF METHODS FOR IMPROVING THE AVAILABILITY OF INFORMATION IN AUTOMATED AUGMENTED REALITY SYSTEMS

Authors: *Wu Liming, master; Turty M.V., PhD, Associate Professor, Admiral Makarov National University of Shipbuilding, Mykolaiv, Ukraine*

Criteria for information security in automated systems are to ensure its confidentiality, integrity, accessibility and observability. Modern automated systems are complex systems, the functioning of which is based on the process of obtaining and processing information about the state of the environment, the state of the control object, the state of the automated system itself and the state of the control system. In such systems, there are many data streams received from different systems and transmitted on many different types of information carrier. Information for different recipients of information can also be expressed in different ways.

In the process of development of automated systems (AS), they are improved through the use of new hardware and software, as well as through the introduction of blocks with new functionality. Augmented reality is one of the promising technologies. The availability of information for users of automated augmented reality systems (ASAR) significantly affects the quality of the automated system as a whole, in particular, the speed and the ratio of correct and erroneous actions of operators.

The development and implementation of ASAR is currently the subject of research by many scientists and engineers worldwide [1, 2, 4]. However, the problem of choosing the optimal methods for displaying information in such system has not been solved at present [3, 5].

The purpose of this work is to develop a methodology for selecting the optimal means of visualization of the generalized characteristics of processes in ASAR, taking into account the limited human perception of information.

To achieve this goal it is necessary to solve the following tasks:

– to analyze modern AS and determine the criteria for their classification;

– to analyze the methods of presenting generalized information in AS and to determine the methods that are appropriate for use in ASAR;

– to define criteria and to develop a technique of a choice of optimum means of visualization of the generalized characteristics of processes in ASAR.

Groups of criteria for the classification of automated systems developed in this tesis are represented in fig.1.

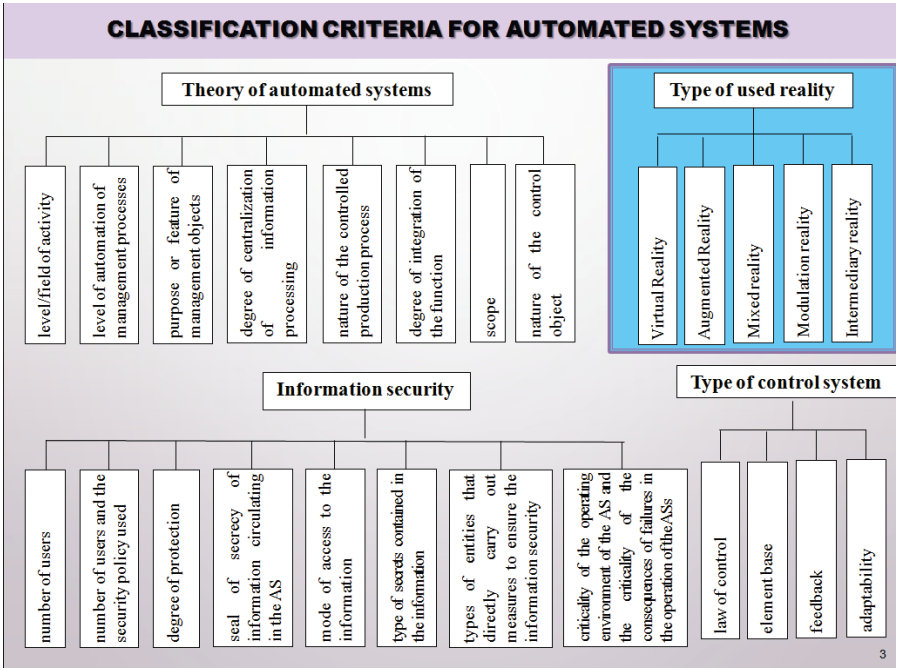


Figure 1 – The classification of automated systems

Information can be presented in various ways and forms. The most common nowadays are textual, graphical and tabular ways of presenting information. Quite often, a combined method is used, which is characterized by the combination of various forms of information presentation. With the development of modern computer technology, a special form of information presentation has appeared – multimedia, which

can combine all of the above methods and forms using dynamic images (animation, video materials) accompanied by audio (sound) information.

Display functions in ASAR systems:

1. Display of information about the current parameters of the system in the form of text, graphs, mnemonic diagrams.

2. Display of graphs of generalized parameters of processes in an automated system in real time for a given time interval.

3. Detection of critical (emergency) situations. Visualization of technological and emergency messages.

4. Archiving of the history of changes in the parameters of the technological process and the control process. Visualization of the history of parameter changes.

5. Operational control of the technological process using tactile screens or virtual control environment.

Dynamically changing information on the display screen, in accordance with its characteristics, can be presented in one of the following forms: in the form of text messages; in the form of numerical values of parameters; in the form of columns of diagrams; in the form of secondary indicating devices (images of devices). The state of the equipment can be displayed in the form of text messages, in the form of objects that change their color and appearance. The state of the technological process can be reflected in the form of text prompts or/and in the form of parts of technological equipment that change their shape and color.

Various equipment can be used to visualize information in automated systems: analog and digital measuring instruments; discrete bar indicator with full scale and scale without filling; smartphones; plates; monitors for personal computers and laptops; control panels of complex AS, containing various devices, screens, sound and light indicators, etc., as well as means for controlling them.

Digital streaming provides information that can be expressed in a variety of ways and transmitted on many different types of media and in a wide variety of systems. These technologies for representing reality include technologies known as augmented reality, augmented reality, mixed reality, and virtual reality. These types of reality, combined with analytics and artificial intelligence, enable the creation of applications that transform physical reality into intelligent reality and help enterprise personnel complete complex tasks.

Augmented reality – projection of any digital information (images, video, text, graphics, etc.) over the screen of any device. As a result, the real world is supplemented with artificial elements and new information. It can be implemented using applications for ordinary smartphones and tablets, augmented reality glasses, stationary screens, projection devices and other technologies.

The number seven constitutes a useful heuristic, reminding us that lists that are much longer than that become significantly harder to remember and process simultaneously [5].

When developing the method we will consider the generalized characteristics of processes in the automated system in the form of the input vector $\mathbf{X}=(x_1, x_2 ..., x_j, ..., x_n)$, where n is the number of parameters to be visualized.

We will create a technique that will allow us to choose the optimal means of visualization of generalized process parameters in automated augmented reality systems among the set of tools $Z=(z_1, z_2 ..., z_i, ..., z_m)$, where m is the number of available visualization tools:

z_1 – numerical (quantitative characteristics) or textual form (qualitative characteristics). In both cases it is a question of output of the text;

z_2 – graph in a parallel coordinate system using the method of interval estimation to convert the vector $\mathbf{X}=(x_1, x_2 ..., x_j, ..., x_n)$ into a set of coordinates $\mathbf{Y}=(y_1, y_2 ..., y_j, ..., y_n)$;

z_3 – T-angle constructed by converting the input vector $\mathbf{X}$ into the set of coordinates of the T-angle $\mathbf{Y}=(y_1, y_2 ..., y_j, ..., y_n)$ [3];

z_4 – T-cell (surface), constructed by converting the input vector $\mathbf{X}$ into the set of coordinates of the T-angle $\mathbf{Y}$;

z_5 – map of the T-angle, constructed by "cutting" the corresponding hypersphere.

In the method we will take into account that:

– the area for visualization of generalized information can be limited (for example, augmented reality glasses), or virtually unlimited (for example, in the case of the use of holographic means for visualization);

– the number of blocks of human-controlled generalized information is limited and depends on the person's qualifications and work experience (the number of these blocks will not exceed 9);

– the size of the symbols and graphs used for visualization must be sufficient for perception by the human eye;

– the presentation of generalized information in the form of diagrams can be carried out using graphs of different types, which have different properties in terms of human perception of information.

Based on the above, the input data include:

– indicator of limited area for visualization of generalized information: $SI = 0$ – unlimited area, $SI = 1$ – limited area. In the latter case, the value of this area SS must be added to the set of input data;

– the minimum value of the area allocated for the display of one symbol $SMINS$;

– the number of characters in each text block of generalized information NC_j;

– the set of chart types $CH = (c_1, c_2 ..., c_k, ..., c_{23})$:

– the set of possible purposes for the visualization of generalized information in the form of charts VP= (v_1, v_2 ..., v_h, ..., v_4): v_1 – Relationships in the data; v_2 – Data distribution; v_3 – Data comparison; v_4 – Data combination;

– the set of types of numerical data that can be represented in the form of charts $DNT = (t_1, t_2 ..., t_g, ..., t_5)$: t_1 – Consecutive numbers; t_2 – Continuous temporary; t_3 – Discrit; t_4 – Geographycal; t_5 – Logical;

– three-dimensional array of recommended types of diagrams for for certain purposes of visualization and data types. If several types of diagrams are recommended, their complexity and clarity can be assessed by a weighted expert assessment. In this case, when deriving the results, these estimates should be reflected in the recommendations.

In the case of using the display of generalized information in the form of interval estimates or T-angles, the upper $y_{j\max}$ and lower $y_{j\min}$ evaluation limits and the criticality score ET_j for each information jth parameter must be specified.

Output data of this technique should be the following data: recommended ways to visualize generalized information in ASAR; explanation of the decision-making procedure at the request of the user; auxiliary illustrations in the process of work; illustrations of user-selected visualization methods; ratings of recommended visualization methods; messages about mistakes made by the user; notification in case of inability to visualize the specified information in the conditions of existing restrictions.

The process of choosing the means of visualization of generalized information in ASAR is proposed to be carried out according to the generalized algorithm fig.2.

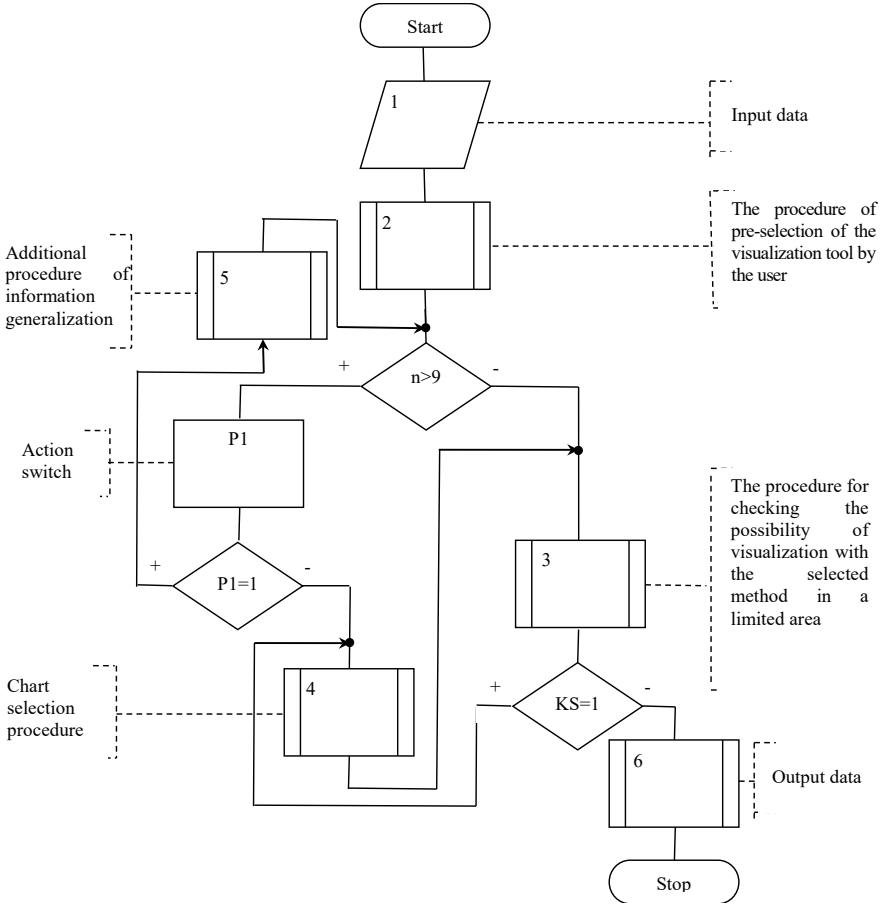


Figure 2 – The generalized algorithm

Conclusions

Thus, in this theses the modern AS and the methods of presenting generalized information in AS have been analyzed; the criteria for classification of automated systems, the methods of presenting generalized information in AS that are appropriate for use in ASAR, the criteria of a choice of optimum means of visualization of the generalized characteristics of processes in ASAR have been determined; the technique of a choice of optimum means of visualization of the generalized characteristics of processes in ASAR have been developed.

References:

1. Data visualization. URL: https://www.salesforce.com/hub/analytics/data-visualization-advantages.

2. Institute of Data Analysis and Visualization. URL: https: www.us1sp.edu/institute-for-data-analytics-and-visualization/

3. Kutkovetsky V.Ya., Turty MV One-dimensional analytical geometry with visualization of clear or unambiguous fuzzy estimates of intellectual solutions // Scientific works: scientific journal. – T.313.-Вип.301. – Mykolaiv: Petro Mohyla National University of Ukraine Publishing House, 2018. – S. 25-30.

4. Meyer A. Improve Productivity through Data Visualization, Dec 16th 2012. URL: https://www workingknowledge.com/blog/improve-productivity-through-data-visualization/

5. Miller, G. A. The magical number seven, plus or minus two: Some limits on our capacity for processing information. /Psychological Review. *63 (2): 81-97.* CiteSeerX 10.1.1.308.8071. doi:10.1037 /h0043158. PMID 13310704. URL: http://psychclassics.yorku.ca/Miller/

УДК 004.056:623.618

DESIGN OF INTEGRATED NAVIGATION FOR UNDERWATER VEHICLE WITH MULTIPLE SENSOR INFORMATION FUSION

Author: *Xue Chenglei, Admiral Makarov National University of Shipbuilding, Mykolayiv, Ukraine*

Scientific adviser: *Turty M.V., PhD, Associate Professor, Admiral Makarov National University of Shipbuilding, Mykolaiv, Ukraine*

Underwater vehicle (AUV – Autonomous Underwater Vehicle) is an integrated system that is intelligent, autonomous, and capable of optimizing the combination of modules according to mission requirements, and realizing multiple functions. There are a wide range of application requirements. When the AUV is performing its mission, it can use the information provided by the inertial navigation system and other navigation equipment such as Doppler (DVL – Doppler Velocity Log), Global Position System (GPS – Global Position System) for navigation and positioning.

The positioning procedure based on combining information from several sensors is similar to the procedure of multi factor identification in access control systems for information resources. The information from each sensor is generally transmitted via its own information transmission channel. Different interferences may occur in each channel, as a result of which the information from the sensors may be distorted. In addition, an attacker can intentionally distort the information in the channel of its transmission, if he gets authorized access to this channel. Positioning based on distorted data would be incorrect. Positioning errors can also be caused by system debugging errors or unintentional operator errors. To determine the optimal version of an integrated navigation system, it is advisable to check its effectiveness on a mathematical model.

The purpose of this work is to increase the capabilities and accuracy of the autonomous integrated navigation system of the underwater vehicle by selecting the optimal structure of the system based on the results of mathematical modeling.

To achieve this goal it is necessary to solve the following tasks:

– to develop a multi-sensory integrated navigation scheme based on the theory of information merging;

– to develop and test a mathematical model that corresponds to the developed scheme.

The model of information merging for the integrated navigation system will be created on the basis of error equations SINS, DVL, LBL and other sensors.

SINS – (Strap-down Inertial Navigation System) uses the inertial information provided by the gyroscope and accelerometer to conduct navigation positioning. The navigation positioning error gradually accumulates with time [1]. DVL can measure the speed of the AUV carrier coordinate system, and has the characteristic that the measurement error does not increase and accumulate over time. It can be useful for correction the speed measurement error of SINS in real time [2], but it cannot eliminate the position measurement error. GPS provides speed and position information with high accuracy [3], but its dynamic performance is poor, and it requires AUV to surface intermittently, which is not conducive to its concealment. The long base line system (LBL-Long Base Line) uses the distance information between the underwater target and the seafloor array to solve the target position, which has the advantages of high relative accuracy and long range [4].

In this article, it is proposed to form and investigate a multi-sensor navigation system consisting of SINS, DVL, LBL, depth gauge and course sensor, using the theory of combined filtering in combining information. This should be able to effectively overcome the shortcomings of a single sensor, address differences in the output frequencies of the sensors, and effectively improve the navigation accuracy of AUV.

The federated filter designed in this paper is a two-stage data fusion structure, and the sub-filter and the main filter work in parallel. As shown in Figure 1, SINS is a public reference system, combined with Doppler speedometer, LBL, magnetic heading, and depth meter to form two sub-filters. The output frequency of each sub-filter that participates in the fusion is different in the actual system, so when designing the filter, the non-equal interval federated filtering algorithm is used to make the main filter can not be simultaneously in the non-fusion period.

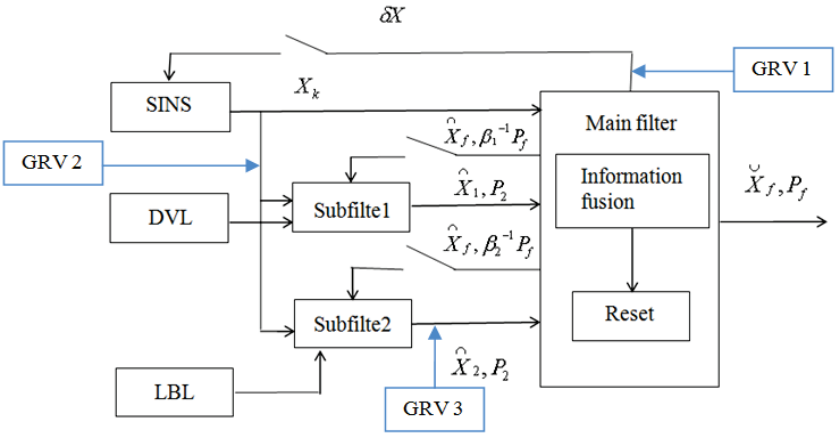


Figure 1 – The general structure of a federated filter

When fusing all the local filter information, each local filter is added to measure the "innovation" to avoid the loss of "innovation" and artificially introduce algorithm errors to achieve the global optimum.

Determining the degree of influence of distortions of information in the channels of its transmission on the efficiency of the integrated navigation system can be carried out by the Monte Carlo method, for which the information transmission channels include generators of random variables (GRV). It is proposed to perform a virtual statistical experiment for the best signal transmission conditions (all random variable generators do not work), for the worst signal transmission conditions (all random variable generators work) and for intermediate cases (for different combinations of working random variable generators).

The MATLAB simulation experiment is carried out for the above model. In case the best signal transmission conditions the simulation conditions are:

1. The AUV is at a depth of 20m in the water, with a heading angle of 45° and a speed of 8 m/s.

2. The relative time of the Doppler velocimeter is 300 s, the output data frequency is 1 Hz, and the velocity error in the *x*, *y*, and *z* directions is

$$\delta V_{dx}(0) = \delta V_{dy}(0) = 0.01 \text{ m/s}.$$

3. The long baseline positioning system seabed transponder has a baseline distance of 1 000 m, an output period of 10 s, and a positioning accuracy of 10 m;

4. The output cycle of the heading sensor is 0.12 s, and the heading measurement accuracy is 0.3;

5. Initial state value of voyage:

Latitude $L(0) = 24^{\circ}30'$.

Longitude $\lambda(0) = 102^{\circ}30'$.

SINS

$$\delta\phi_N(0) = \delta\phi_N(0) = \delta\phi_E(0) = 5';$$
$$\delta V_N(0) = \delta V_U(0) = \delta V_E(0) = 0.01\, m/s;$$
$$\delta L(0) = \delta\lambda(0) = 10/\mathrm{Re}, \delta h(0) = 0.1\, m;$$
$$\mathrm{E}_{dx}(0) = \mathrm{E}_{dy}(0) = \mathrm{E}_{dz}(0) = 0.02\ ^{\circ}/h;$$
$$\Delta_{dx}(0) = \Delta_{dy}(0) = \Delta_{dz}(0) = 100\ \mu g.$$

6. The constant drift of the laser gyroscope is 0.02°/h, and the zero offset of the accelerometer is 1×10^{-3} g.

7. Initial *P* selection for each sub-filter

$$P_{10} = 100 \times \mathrm{diag}[(5')^2,(5')^2,(5')^2,(0.01m/s)^2,$$
$$(0.01m/s)^2,(0.01m/s)^2,(\frac{10}{\mathrm{Re}}m)^2,(\frac{10}{\mathrm{Re}}m)^2,$$
$$(0.1m)^2,(0.01^{\circ}/h)^2,(0.01^{\circ}/h)^2,(0.01^{\circ}/h)^2,$$
$$(100\mu g)^2,(100\mu g)^2,(100\mu g)^2,(0.03m/s)^2,$$
$$(0.03m/s)^2,(0.03m/s)^2];$$
$$P_{20} = 100 \times \mathrm{diag}[(5')^2,(5')^2,(5')^2,(0.01m/s)^2$$
$$(0.01m/s)^2,(0.01m/s)^2,(\frac{10}{\mathrm{Re}}m)^2,(\frac{10}{\mathrm{Re}}m)^2,$$
$$(0.1m)^2,(0.01^{\circ}/h)^2,(0.01^{\circ}/h)^2,(0.01^{\circ}/h)^2,$$
$$(100\mu g)^2,(100\mu g)^2,(100\mu g)^2].$$

The calculation period of SINS is 20 ms. The information fusion period of all sub-filters takes the least common multiple of the output period of each sensor as 1 s. The main filter has no time update and measurement update process, and the global estimation only fuses the common state output by the local filter. The feedback status includes: misalignment angle, speed error, and position error. The simulation time is 600 s, and the real-time correction of the navigation parameters is carried out after the filter starts 20 s. As shown in Figure 2, the curve is the residual error after the combined navigation system uses the filter value of the federal filter to compensate the SINS error (that is, the filter error).

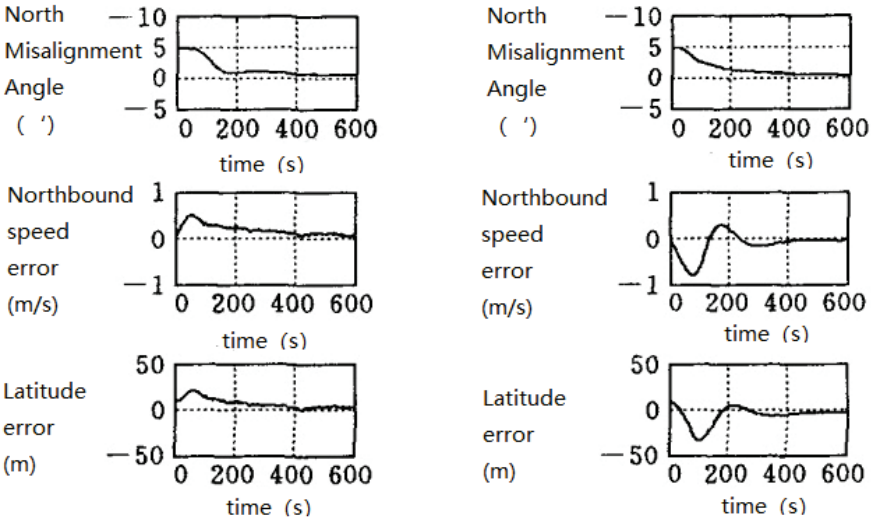


Figure 2 – Attitude, velocity error, and position error estimation after federated filtering

Generally speaking, it is difficult for the SINS/DVL integrated navigation system to correct the position error. It can be seen from Figure 2 that the introduction of LBL in this system makes the latitude and longitude error rapidly reduce and converge, and the non-equal interval filtering algo-

rithm of the federated filter is used to solve the problem. The output information of each sensor is different. It can be seen from the simulation results that the designed federated filter has significant effects and can meet the requirements of the system for high-precision positioning [5].

Conclusion

In this thesis, a multi-sensory integrated navigation scheme based on the theory of information merging have been developed, a mathematical model that corresponds to the developed scheme have been developed and tested. The simulation results for integrated navigation system scheme based on multi-sensor information fusion technology that uses federated filtering technology to fuse DVL\LBL\ heading sensor\ depth gauge, and solves the difference in output cycle of each sensor during fusion show that the program makes full use of the information of various navigation sensors to achieve the best overall performance of the system and effectively improve the navigation positioning accuracy of the AUV.

References:

1. Titterton D.H, Weston J.L. Strapdown Inertial Navigation Technology. – London: Peter Pegerinus, 1997. – P.392.
2. Lee C.,Lee P., Hong S.,et al. Underwater Navigation System based on An Intertial Sensor and Doppler Velocity Loguesing Indirect Feedback Kalman Filter // Offshore and Polar Engineering. – 2005. – No.15(2). – PP.88-95.
3. Marco D.B., Healey A.J. Comm and Control, and Navigation Experimental Results with the NPS ARIESAUV // Oceanic Enginering. – 2001. – No.26 (24). – PP.466-476.
4. Daxiong J., Xiao zhen C., Yiping L., et al. Analysis of several problems in the marine application of the AUV long base line system // Ocean Engineering. – 2007. – No.25(4). – PP.92-95.
5. Lee P., Jeon B., Kim S., et a1. Simulation of an Inertial Acoustic Navigation System With Range Aiding for an Autonomous Underwater Vehicle // Journal of Oceanic Engineering. 2007. – No.32(2). – PP.327-344.

УДК 004.056.5

НОРМАТИВНО ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ, РОЗРОБКА КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ НА ОБ'ЄКТІ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ В НАЦІОНАЛЬНІЙ ГВАРДІЇ УКРАЇНИ

Автор: *Пивоваров І.М., Військова частина 3039 Національної гвардії України, магістрант, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

Науковий керівник: *Турти М.В., к.т.н., доцент, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

Актуальність даної роботи обумовлена збільшенням об'єктів інформаційної діяльності третьої категорії, де озвучується інформація з обмеженим доступом (ІзОД) у військових частинах Національної гвардії України (НГУ), де необхідно створювати комплекс технічного захисту інформації (КТЗІ).

Створення КТЗІ базується на великій кількості нормативно-правових актів [1], опрацювання яких доцільно уніфікувати і автоматизувати [2].

Метою даної роботи є оптимізація та спрощення проведення робіт зі створення передпроектної документації у військових частинах.

Для досягнення цієї мети необхідно:

– визначити нормативно-правову базу створення КТЗІ в НГУ;

– провести аналіз вимог нормативно-правових документів у сфері технічного захисту інформації (ТЗІ), наказів і методичних вказівок, що регламентують діяльність служби ТЗІ в НГУ;

– розробити шаблон комплексної системи захисту інформації на об'єкті інформаційної діяльності в НГУ відповідно до визначених вимог.

Метою створення КТЗІ є захист ІзОД під час проведення нарад з питань службової діяльності військової частини, документальної ІзОД під час роботи з документами, мовної ІзОД під час проведення телефонних переговорів засобами зв'язку від загроз порушення конфіденційності, цілісності та доступності інформації.

Головними завданнями створення КТЗІ є: блокування технічних каналів витоку інформації, шляхів несанкціонованого доступу та загроз для ІзОД.

Для досягнення цієї мети необхідно проаналізувати нормативно правове забезпечення в сфері технічного захисту інформації, організаційні документи і накази в структурі НГУ та розробити шаблони наступних документів:

– акт категоріювання об'єкта інформаційної діяльності;

– акт обстеження об'єкта інформаційної діяльності та інженерного аналізу допоміжних технічних засобів та систем;

– модель загроз для інформації з обмеженим доступом, яка циркулює на об'єкті інформаційної діяльності;

– технічне завдання на створення комплексу технічного захисту інформації на об'єкті інформаційної діяльності;

– технічний проект (пояснювальна записка з ТЗІ)

– паспорт комплексу технічного захисту інформації на об'єкт інформаційної діяльності.

Перелік нормативно правових документів згідно яких повинен розроблятися комплекс технічного захисту інформації на об'єкті інформаційної діяльності;

– Положення про технічний захист інформації в Україні, затверджене Указом Президента України від 27.09.1999 № 1229;

– Порядок організації та забезпечення режиму секретності в державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях, затверджений постановою Кабінету Міністрів України від 18.12.2013 № 939;

– Положення про захист інформації від витоку технічними каналами на об'єктах інформаційної діяльності та в інформаційно-телекомунікаційних системах, затверджене наказом Адміністрації Держспецзв'язку України від 19.06.2015 № 023;

– ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації. Основні положення;

– ДСТУ 3396.1-96. Захист інформації. Технічний захист інформації. Порядок проведення робіт;

– ДБН А.2.2-2-96. Технічний захист інформації. Загальні вимоги до організації проектування і проектної документації для будівництва;

– Модель технічних розвідок ТР-2030, затверджена наказом Адміністрації Держспецзв'язку від 30.12.2015 № 153/ДСК;

– НД ТЗІ 1.6-006-2015 Положення про категоріювання об'єктів інформаційної діяльності;

– НД ТЗІ 1.6-003-04. Створення комплексів технічного захисту інформації на об'єктах інформаційної діяльності. Правила розроблення, побудови, викладення та оформлення моделі загроз для інформації;

– НД ТЗІ 3.6-003-2016. Порядок проведення робіт зі створення та атестації комплексів технічного захисту інформації;

– НД ТЗІ 2.2-009-2015 Норми ефективності захисту інформації, яка озвучується на об'єктах інформаційної діяльності, від витоку лазерного акустичними каналами (із змінами);

– НД ТЗІ 2.3-020-2015 Методика контролю захищеності інформації, яка озвучується на об'єктах інформаційної діяльності, від витоку лазерними акустичними каналами (із змінами);

– НД ТЗІ 2.4-011-2015 Вимоги та рекомендації із захисту інформації, яка озвучується на об'єктах інформаційної діяльності, від витоку лазерними акустичними каналами;

– НД ТЗІ 2.2-004-06Протидіятехнічнимрозвідкам. Норми з протидії засобам фотографічної та оптико-електронної розвідок.

– НД ТЗІ 2.3-011-06 Протидія технічним розвідкам. Методики контролю виконання норм з протидії засобам фотографічної та оптико-електронної розвідок.

– НД ТЗІ 2.2-008-2015 Норми ефективності захисту інформації, яка озвучується на об'єктах інформаційної діяльності, від витоку акустичними та віброакустичними каналами;

– НД ТЗІ 2.3-019-2015 Методика контролю захисту інформації, яка озвучується на об'єктах інформаційної діяльності, від витоку акустичними та віброакустичними каналами;

– НД ТЗІ 2.4-010-2015 Вимоги та рекомендації із захисту інформації, яка озвучується на об'єктах інформаційної діяльності, від витоку акустичними та віброакустичними каналами;

– НД 3.6-003-20116 Порядок проведення робіт зі створення та атестації комплексів технічного захисту інформації.

– Нормы эффективности защиты технических средств передачи речевой информации от утечки за счет побочных излучений и наводок, ГТК СССР № 13 26.09.1977.

Висновки

Таким чином, в даній роботі на основі проведеного аналізу нормативно-правової документації у сфері технічного захисту інформації та відповідних наказів і методичних вказівок створено шаблон для потреб Національної гвардії України, який доцільний для використання підрозділами ТЗІ у військових частинах.

Список літератури:

1. Перун Т. Методологічні засади дослідження механізму забезпечення інформаційної безпеки в Україні //Вісник Національного університету «Львівська політехніка». Серія: Юридичні науки. – 2017. – № 865. – С 303-307.

2. Турти, М. В. Розробка блоку прийняття рішень для АСОД ДССЗЗІ / М. В. Турти, С. М. Нужний, А. П. Гунченко // Вісник Національного університету "Львівська політехніка". Автоматика, вимірювання та керування. – 2016. – № 852. – С. 99-105.

СЕКЦІЯ 4. ПІДГОТОВКА КАДРІВ У ГАЛУЗІ ЗНАНЬ «ІНФОРМАЦІЙНА БЕЗПЕКА»

УДК 004.891.2

АНАЛІЗ ОСОБЛИВОСТЕЙ КАНАЛІВ ВИТОКУ ІНФОРМАЦІЇ ДЛЯ ОБ'ЄКТІВ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ГВАРДІЇ УКРАЇНИ

Автор: *Грищенко О.М., Головне управління Національної гвардії України, м. Київ, Україна, магістрант, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

Науковий керівник: *Нужний С.М., к.т.н., доцент, зав. каф. КТІБ, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

Всі громадяни України, юридичні особи і державні органи мають право на інформацію, що передбачає можливість вільного одержання, використання, поширення та зберігання відомостей, необхідних їм для реалізації ними своїх прав, свобод і законних інтересів, здійснення завдань і функцій. Кожному громадянину забезпечується вільний доступ до інформації, яка стосується його особисто, крім випадків, передбачених законами України.

Незаконні інформаційні потоки створюють витік інформації і, тим самим, реалізуються загрози безпеці інформації з обмеженим доступом (ІзОД) на ОІД підприємства.

Зрозуміло, що необхідно контролювати по можливості всі відомі канали витоку [1].

Найбільш загальною класифікацією каналів витоку інформації може бути:

– несанкціонований доступ (НСД);

– канал спеціального недопустимого регламентом впливу на параметри середовища функціонування;

– канал спеціального впливу нештатними програмними та/або програмно-технічними засобами на елементи обладнання;

– канал спеціального впливу на ОІД за допомогою закладених пристроїв;

– канал витоку інформації, утворений за допомогою використання інформативних параметрів ПЕМВН;

Рисунок 1 – Класифікація інформації у відповідності до Закону України «Про інформацію»

– канал витоку інформації, утворений за допомогою використання побічних акустоелектричних перетворень інформативних сигналів;

– канал утворений за рахунок використання випадкових збоїв та відмов в роботі обладнання;

– канал спеціального впливу на компоненти АС за допомогою впровадження комп'ютерних вірусів.

Перекриття всіх можливих каналів несанкціонованого знімання інформації вимагає значних витрат, і, тому, у повному обсязі зробити це вдається далеко не завжди.

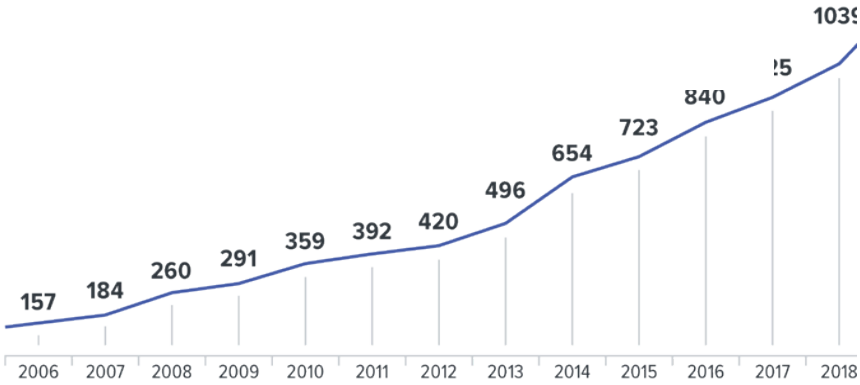


Рисунок 2 – Число зареєстрованих витоків інформації у світі.

Основними причинами витоку інформації є [2]:

– недотримання особовим складом організаційних норм, вимог та правил;

– помилки в проектуванні ОІД і систем захисту АС;

– ведення технічної і агентурної розвідок.

Причини витоку ІзОД досить тісно пов'язані з видами витоку інформації. Відповідно до керівних документів в галузі ТЗІ розглядаються три види витоку інформації:

– розголошення;
– несанкціонований доступ до інформації;
– одержання розвідками захищеної інформації.
– можна визначити першочергові завдання зі забезпечення безпеки інформації (рис. 3).

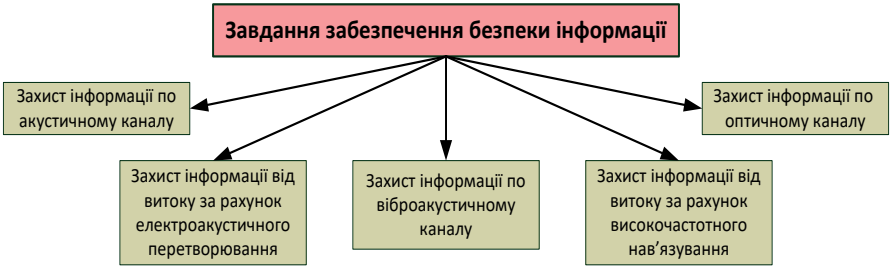


Рисунок 3 – Завдання забезпечення безпеки інформації в приміщенні для проведення нарад

Таблиця 1 – Технічні канали витоку інформації

На базі засобів пасивного перехоплення	**На базі засобів активного перехоплення**
За рахунок інформативних побічних електромагнітних випромінювань і наведень	З використанням технічних заставних пристроїв
З використанням спеціальних керованих мікрофонів	З використанням лазерних пристроїв, що підслухують
За рахунок електроакустичних перетворень	За рахунок прямої реєстрації інформаційних сигналів з наступною передачею по радіоканалі
За рахунок прямої реєстрації інформаційних сигналів	За рахунок низько- та високочастотних сигналів на технічні засоби (за рахунок нав'язування)
З використанням апаратури фотографування	

Класифікація акустичних сигналів:
– *Тональний* – це сигнал, що викликаний коливанням, яке відбувається за синусоїдальним законом.

– *Складний* сигнал включає цілий спектр гармонійних складових.

– *Мовний* сигнал є складним акустичним сигналом у діапазоні частот від 200...300 Гц до 4...6 кГц [3]..

Класифікація методів доступу несанкціонованого доступу до ІзОД в акустичному каналу витоку інформації представлена на рис.4.

Рисунок 4 – Несанкціонований доступ до конфіденційної інформації з акустичного каналу

Висновки

Безпосереднє вдосконалення як технологій, так і засобів негласного знімання мовної інформації, що підтверджується зростаючими витратами на розробку і виробництво відповідної апаратури, потребує, згідно з логікою організації протидії, певної уваги до методів і засобів захисту.

Щоб гарантувати високу ступінь захисту мовної інформації, необхідно постійно вирішувати складні науково-технічні завдання щодо розробки та вдосконалення засобів і способів захисту. Комплексні рішення таких завдань дозволяють уникнути хибних ситуацій, коли один з елементів системи має вади, а інші не зможуть у потрібний час протистояти загрозам навіть у випадку значного підсилення їх захисних властивостей.

Список літератури:

1. Защита выделенных помещений [Электронный ресурс] // Особистий web-сайт http://security.to.kg/lib/vydelen.htm.
2. Бузов Г.А., Защита от утечки информации по техническим каналам[Текст]. Г. А. Бузов. – М., 2005 г.
3. Микроэлектронные устройства автоматики: Учеб. пособие для вузов / А.А. Сазонов, А.Ю. Лукичев, В.Т. Николаев и др.; Под ред. А.А. Сазонова. – М.: Энергоатомиздат, 1991. – 384 с.: ил.
4. Хорев А.А. Защита информации от утечки по техническим каналам. Часть 1. Технические каналы утечки информации. Учебное пособие. М.: Гостехкомиссия России, 1998. – 320 с.
5. Волокітін А.В., Маношкин А.П., Солдатенков А.В., Савченко С.А., Петров Ю.А. Інформаційна безпека державних організацій і комерційних фірм. Довідковий посібник (під загальною редакцією Реймана Л.Д.) М.: НТЦ “ФИОРД-ИНФО”, 2002р.

УДК 004.056.05

ДОСЛІДЖЕННЯ ВРАЗЛИВОСТЕЙ ЛАБОРАТОРНОЇ КОМП’ЮТЕРНОЇ СИСТЕМИ ЗА ДОПОМОГОЮ ЕКСПЛОЙТІВ

Автор: *Жагліна А.І., Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

Науковий керівник: *Турти М.В., к.т.н., доцент, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

Як зазначено в Стратегії кібербезпеки України «XXI століття знаменується активним формуванням шостого технологічного укладу та ризиками, з якими стикається цивілізація внаслідок упровадження новітніх технологій. Питома вага кіберзагроз зростає і ця тенденція в

міру розвитку інформаційних технологій та їх конвергенції з технологіями штучного інтелекту в найближче десятиліття посилюватиметься» [1]. Найсучаснішими є засоби і методи хакінгу, які застосовуються у сфері шпигунства у кіберпросторі, як і контрзаходи, призначені для боротьби з ними.

Необхідною умовою успішного захисту інформаційних ресурсів від дій зловмисників у кіберпросторі є системний підхід до аналізу мережевого хакінгу. Він охоплює всі етапи підготовки та реалізації атак з боку зловмисника (збирання даних, проникнення в систему, несанкціоновані операції із цінною інформацією) і етапи підготовки та функціонування системи захисту (аналіз процесів обігу інформації на об'єктах інформаційної діяльності; аналіз трендів технологій обробки і захисту інформації; аналіз трендів технологій порушення інформаційної безпеки зловмисниками; виявлення поточних і прогнозованих вразливостей і актуальних загроз; планування реакції системи захисту на дії зловмисника; розробка, впровадження, експлуатація, модернізація комплексної системи захисту інформації) у певному середовищі функціонування системи з врахуванням його прогнозованих змін.

Ступінь захищеності комп'ютера багато в чому залежить від досконалості його операційної системи. Операційна система (ОС) є найважливішим програмним компонентом будь-якої електронної обчислювальної машини, тому від рівня реалізації політики безпеки в кожній конкретній ОС багато в чому залежить і загальна безпека інформаційної системи.

Проблеми вразливості операційної є предметом дослідження багатьох вітчизняних і зарубіжних науковців і практиків [2-9]. Фахівець з кібербезпеки має аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційних ресурсів згідно з встановленою політикою інформаційної та/або кібербезпеки. Однак, навіть при високій насиченості лабораторій навчального закладу обчислювальною технікою, формування такого результату навчання ускладняється застосовуваною в комп'ютерних класах політикою безпеки, згідно з якою користувачі групи «Студент» найчастіше не мають прав доступу для налагодження персонального комп'ютера (ПК), інсталяції/деінсталяції програмного

забезпечення, налагодження ОС. Тому актуальною задачею є розробка спеціалізованого лабораторного стенду, призначеного для проведення досліджень і здобуття студентами практичних навичок пошуку і нейтралізації вразливостей найбільш розповсюджених інформаційних технологій та ОС.

Метою даної роботи є виявлення вразливостей лабораторної комп'ютерної системи на основі операційної системи Windows за допомогою експлойтів.

Для досягнення поставленої мети необхідно розв'язати наступні задачі:

– провести аналіз стратегій зловмисників використання вразливостей ОС Windows і відповідних стратегій протидії ним служби захисту інформації;

– визначити функціональний склад, структуру і апаратно-програмне забезпечення лабораторного стенду для пошуку і нейтралізації вразливостей операційної системи Windows;

– провести апробацію розробленого стенду на віртуальних ОС.

Висновки

В ході виконання даної роботи було проведено аналіз стратегій зловмисників з використання вразливостей ОС Windows і відповідних стратегій протидії ним служби захисту інформації; визначено функціональний склад, структуру і апаратно-програмне забезпечення лабораторного стенду; проведено апробацію розробленого стенду на віртуальних ОС.

Список літератури:

1. Стратегія кібербезпеки України, затверджена Указом Президента України №447/2021 від 14 травня 2021 року «Про рішення Ради національної безпеки і оборони України "Про Стратегію кібербезпеки України"». URL: https://www.president.gov.ua/documents/4472021-40013

2. Exploits and exploit kits. URL: https://docs.microsoft.com/en-us/windows/security/threat-protection/intelligence/exploits-malware

3. Взлёты и падения рынка эксплойтов. URL: https://habr.com/ru/company/trendmicro/blog/570282/

4. Новая уязвимость в Windows позволяет легко получить права администратора. URL: https://www.ixbt.com/news/2021/11/24/novaja-ujazvimost-v-windows-pozvoljaet-legko-poluchit-prava-administratora.html

5. Нефедова М. Опубликован эксплоит для Windows, позволяющий повысить права до уровня администратора. URL: https://xakep.ru/2021/11/23/0day-lpe/
6. Одна из разработок NSO Group оказалась «элитным» шпионским инструментом. URL: https://www.securitylab.ru/news/527694.php/
7. Советы Microsoft. URL: https://www.cnews.ru/news/top/2020-0113_microsoft_predlozhila_ 400_ mln_polzovatelej
8. Ільєнко А.В., Ільєнко С.С., Куліш Т.М. Перспективні методи захисту операційної системи Windows // Кібербезпека: освіта, наука, техніка. – 2020. – №4(8). – С.124-132. URL: https://www.researchgate.net/publication/342448471_PERSPEKTIVNI_METODI_ZAHISTU_OPERACIJNOI_SISTEMI_WINDOWS
9. Ільєнко А.В., Ільєнко С.С., Куліш Т.М. Програмний метод захисту операційної системи Windows на базі технології Blockchain. URL: https://conf.ztu.edu.ua/wp-content/uploads/2021/05/45-2.pdf
10. Козачок В.А, Бурячок Л.В., Складанний П.М. Пентестінг як інструмент комплексної оцінки ефективності захисту інформації в розподілених корпоративних мережах // Сучасний захист інформації. – К.: Державний ун-т телекомунікацій, 2015. – №3 – С.4–12.

УДК 001.92:321.7

ВИКОРИСТАННЯ CLOUD COMPUTING У ПІДГОТОВЦІ ФАХІВЦІВ З ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Автор: *Шуляк Н.О., аспірант, Волинський національний університет імені Лесі Українки, м. Луцьк, Україна*

Актуальність теми дослідження пов’язана з тим, що за умов упровадження інформаційно-комунікаційних технологій у навчальний процес вищого навчального закладу особливого значення набувають завдання створення його інформаційного простору. Слід відзначити взаємопов’язані процеси розвитку апаратно-програмних складових ІКТ і розробки нових комп’ютерно-орієнтованих систем навчання. Враховуючи такі тенденції, можна стверджувати, що інформаційно-освітній простір ВНЗ має бути динамічним утворенням.

Сьогодні без використання сучасних інформаційних технологій не може ефективно працювати жоден освітній заклад. При цьому зміст і розвиток власної IT-інфраструктури при кожному освітньому центрі обходиться дуже дорого. З кожним роком рівень таких витрат все більше і більше зростає. Установи витрачають великі суми на комп'ютерну техніку, телекомунікаційне обладнання та програмне забезпечення. Також значні фінансові вкладення потрібні і для підтримки високого рівня професіоналізму цих співробітників.

Існуюча система освіти перестала влаштовувати практично всі держави світу і піддається активному реформуванню в наші дні. Перспективним напрямом використання в навчальному процесі є нова інформаційна технологія, яка дістала назву хмарні обчислення (англ. – Cloud computing). Концепція хмарних обчислень стала результатом еволюційного розвитку інформаційних технологій за останні десятиліття. Протягом декількох років хмарні сервіси змінили сприйняття та використання інформаційних технологій як для підприємств так і для освітніх закладів, але в той же час, це лише початок їх розвитку.

Одним із найважливіших завдань вищих навчальних закладів у сфері підготовки кадрів з інформаційної безпеки є інфоосвіта та підготовка професійних кадрів для інформаційно-аналітичної галузі. Сучасний швидкий поступ інформаційних технологій вимагає якісно нових освітніх послуг для забезпечення гідного рівня підготовки фахівців у різних галузях життєдіяльності суспільства [1].

Аспектом освітнього завдання є комп'ютерна грамотність населення, яку можна підвищити за допомогою зусиль середньої школи. Інформатизація шкіл, навчального процесу повинна стати, крім всього іншого, квінтесенцією сучасної шкільної реформи. Бажано впроваджувати інформаційні, мультимедійні технології в навчальний процес з усіх шкільних предметів, а не просто організувати комп'ютерні класи в школах [2].

З кожним роком рівень таких витрат все більше і більше зростає. Установи витрачають великі суми на комп'ютерну техніку, телекомунікаційне обладнання та програмне забезпечення. Також значні фінансові вкладення потрібні і для підтримки високого рівня професіоналізму цих співробітників. Існуюча система освіти перестала влаштовувати практично всі держави світу і піддається активному

реформуванню в наші дні. Перспективним напрямом використання в навчальному процесі є нова інформаційна технологія, яка дістала назву хмарні обчислення *(англ. – Cloud computing)*. Концепція хмарних обчислень стала результатом еволюційного розвитку інформаційних технологій за останні десятиліття. Протягом декількох років хмарні сервіси змінили сприйняття та використання інформаційних технологій як для підприємств так і для освітніх закладів, але в той же час, це лише початок їх розвитку [3].

У сучасній науковій літературі найчастіше зустрічається поділ «хмарних систем» за типом архітектури та наданням послуг на: IaaS – інфраструктура як послуга, Paas – платформа як послуга та SaaS – програмне забезпечення як сервіс. Крім того, також виділяють 4 моделі розгортання "хмар" [4]:

– приватні «хмари» – це модель, за якої інфраструктура експлуатується виключно для організації і може перебувати під контролем організації, або третьої сторони;

– «хмари» спільноти – хмари інфраструктури є загальними для декількох організацій, які поділяють відповідальність (наприклад, щодо адміністрування, вимог безпеки, політики розвитку);

– громадські «хмари», інфраструктура яких стає доступною для широкої громадськості, або великої групи організацій і є власністю суб'єкта продажу «хмарних» сервісів;

– гібридні «хмари», що є поєднанням двох або більше «хмар» (приватні, громадські або державні), які пов'язані між собою за допомогою стандартизованих, або власних технологій для взаємного використання даних і додатків.

– Хмарні сервіси освіти за допомогою інформаційно-комунікаційних технологій та інформаційних ресурсів досконаліші, ніж ті, що надаються через VLE-системи. Йдеться про кращу якість інструментів для генерації користувацького контенту і інтеграції з соціальними мережами, персоналізацію за допомогою таких інструментів, як iGoogle, на базі Google Personal Start Page. Так, Google ввів в експлуатацію API для «Apps для навчальних закладів», що дозволяє освітнім установам налаштовувати прикладні програми і

інтегрувати додаткове програмне забезпечення, причому відомості віджету будуть доставлятися з внутрішніх систем навчального закладу. Google Wave є системою для спільної роботи, де по'єднуються концепції електронної пошти, сервісу миттєвих повідомлень, форуму та соціальної мережі. Вона є функціональною моделлю для віджетів, що розміщуються в хмарі, але інтегрованих на різних платформах, включаючи мобільні пристрої.

Список літератури:

1. А.Митко Застосування інформаційно-комунікаційних технологій у підготовці кадрів для інформаційно-аналітичної та політичної сфер, *Інформаційні технології і засоби навчання*. 2018. № 65(3). с. 291-303.

2. O. Sosnin, "Information sphere in the realization of the interests of innovative development of the nation", *Journal of the Verkhovna Rada of Ukraine "Veche"*. [Electronic resource]. Available at: http:// www.viche.info/journal/2675/.

3. А.Митко Переваги та загрози використання сервісу «академічна хмара» у навчальній діяльності вищих навчальних закладів. *Міжнародні відносини, суспільні комунікації та регіональні студії.* Луцьк: Вежа-Друк, 2018. №1 (3). С.60-66.

4. Н. Склатер, «Электронное образование в облаке*». 10-й международный журнал по проблемам систем управления виртуальным и индивидуальным обучением*. 1(1). 10-19, Январь-Март 2010.

СЕКЦІЯ 5. ШКОЛА МОЛОДИХ НАУКОВЦІВ

УДК 004.056

КИБЕРБЕЗОПАСНОСТЬ НА ФЛОТЕ

Автор: *Дзюбас Д.С., Национальный университет кораблестроения имени адмирала Макарова, г. Николаев, Украина*

Научный руководитель: *Турты М.В., к.т.н., доцент, Национальный университет кораблестроения имени адмирала Макарова, г. Николаев, Украина*

Согласно отчету Eropean Network and Information Security Agency (ENISA) [1] «Analys is of cybersecurity aspects in the maritime sector» (ноябрь 2016 года), «озадаченность вопросами кибербезопасности в морском секторе находится на низком уровне либо вообще отсутствует».

Недостаточное внимание к вопросам, связанным с киберугрозами, отмечают и аналитики компании Cyber Keel [2], специализирующейся на безопасности морской индустрии. Они отмечают тот факт, что многие занятые в морской сфере привыкли быть частью «практически невидимой» отрасли, поскольку, «чаще всего, если обычный человек не живет около значительного порта, он не может представить себе действительных масштабов всей индустрии».

«Зависимость морской индустрии от технологий также представляет риски. Подверженность кибератакам (помимо утраты данных) растет. Уже имел место ряд значимых киберинцидентов, и развитие технологий, включая Интернет и электронную навигацию, означает, что в распоряжении отрасли всего несколько лет, чтобы подготовиться к риску утраты судов в результате кибератак. «Пираты уже злоупотребляют наличием прорех в системе кибербезопасности для планирования кражи конкретных грузов» – говорится в отчете Allianz о безопасности судоходства за 2017 год.

Вопрос дополнительно осложняется тем, что, по данным Reuters, далеко не вся информация об успешно проведенных атаках получает широкую огласку, поскольку владельцы бизнеса могут опасаться та-

ких последствий разглашения, как потеря имиджа, претензии со стороны клиентов и страховых компаний, начало расследований, проводимых сторонними организациями и государственными органами.

В последнее время процессы исследования кибербезопасности водно-транспортного комплекса и разработки его методологического и нормативно-правового обеспечения активизировались [1-10].

Целью данной работы является определение тенденций в области кибербезопасности на флоте.

Для достижения поставленной цели не обходимо решить следующие задачи:

– определить наиболее распространенные информационно-коммуникационные системы, (ИКС) используемые в водно-транспортном комплексе и их особенности;

– определить актуальные уязвимости таких систем и возможные последствия нарушения кибербезопасности;

– определить перспективные пути нейтрализации уязвимостей.

Специалисты компании Positive Technologies к основным специфическим для морского транспорта информационным системам и технологиям относят:

– AIS (Automatic Identification System) – автоматическая идентификационная система для передачи идентификационных данных судна (в том числе о его грузе), информации о его состоянии, текущем местоположении и курсе. AIS также используется для предупреждения столкновений судов, мониторинга их состояния, коммуникации между судами, отслеживания судна владельцем. Устройство работает посредством передачи сигналов в УКВ-диапазоне между судами, плавающими ретрансляторами и береговыми AIS-шлюзами, которые подключены к Интернету. Все суда, совершающие международные рейсы, суда водоизмещением более 500 регистровых тонн и все пассажирские суда должны быть оснащены AIS. AIS работает и на морской поисково-спасательной технике.

– ECDIS (Electronic Chart Display and Information System) – электронно-картографическая навигационно-информационная система, которая собирает и использует сообщения AIS, данные с радаров, GPS и прочих судовых датчиков (с гирокомпаса) и сопоставляет их со вшитыми картами. Используется для навигации, автоматизации некото-

рых задач судоводителя и повышения навигационной безопасности мореплавания. ECDIS обычно представляет собой расположенную на мостике судна рабочую станцию (или две — для мониторинга и для планирования курса) под управлением ОС семейства Windows. К рабочей станции с ECDIS, посредством бортовой LAN-сети (чаще всего с доступом в Интернет) подключены другие системы: NAVTEX (навигационный телекс, унифицированная система передачи навигационной, метеорологической и другой информации), AIS, радары и GPS-оборудование, а также другие датчики и сенсоры. До 2019 года ECDIS должны были быть обязательно установить на всех судах;

– VDR (Voyage Data Recorder) – регистратор данных рейса, представляющий собой бортовой самописец, аналог «черного ящика», используемого в авиации. Основные задачи — запись важной рейсовой информации судна, включая как технические и курсовые данные, так и голосовые записи с капитанского мостика, и ее сохранение в случае чрезвычайной ситуации. Данные VDR крайне важны при расследовании инцидентов, аварий и катастроф, произошедших на море;

– TOS (Terminal Operating System) – IT-инфраструктура, служащая целям автоматизации процессов обработки грузов в порту, таких как погрузка и разгрузка, инвентаризация и мониторинг движения по территории порта, оптимизация складирования и поиск нужных в данный момент контейнеров, обеспечение дальнейшего транзита. На практике может являться как целостным продуктом конкретного вендора, так и совокупностью систем, выполняющих различные задачи;

– CTS (Container Tracking System) – система, позволяющая отслеживать движение контейнеров посредством GPS и реже других каналов передачи данных. Аналогичные системы используются также для отслеживания персональных трекеров туристов, автотранспорта и пр.;

– EPIRB (Emergency Position Indicating Radio Beacon) – аварийный радиобуй, передатчик, подающий при активации сигнал бедствия, передача которого в зависимости от технологии исполнения может осуществляться через спутник, в диапазоне УКВ или же комбинированно. Кроме сигнала бедствия некоторые EPIRB могут также передавать информацию о судне (при синхронизации с AIS).

В портах также используются специализированные ИКС:

HAPAG-LLOYD – для регистрации принятия груза на склад, места его размещения и всех перемещений, что позволяет отслеживать статус груза по время погрузки, определять ожидаемое время прибытия груза в порт разгрузки, планировать дальнейшие логистические операции вплоть до доставки груза получателю;

COAST – для оперативного информирования клиентов и руководства порта про местоположение, содержание и состояние груза, правила его обработки и таможенного оформления;

DAKOSY – для организации взаимодействия партнеров в логистических операциях на основе специальной базы данных, содержащей сведения о налоговых декларациях, накладных, экспертных сертификатах, экспедиторских документах, счетах за груз и его транспортировку и различные сообщения, а также позволяющей выставлять счета и проводить платежи в электронной форме, обрабатывать исходные данные и сохранять результаты в файлах с индивидуальным дизайном документации и статистикой. Оформленные один раз документы при помощи модуля SEEDOS (Seaport Forwarders Documentation System), поддерживающего электронный импорт-экспорт документов, локальных сетей и Интернет становятся доступными партнерам (перевозчикам, экспортерам, агентам судоходных компаний, управляющим портовыми терминалами и др.);

ACTION (Agents Container Transport Improving and Organizing Network) – для обслуживания транспортировки контейнеров. Пользователи могут оперативно взаимодействовать с морским, железнодорожным, автомобильным транспортом, получая полный контроль над контейнерными грузами и процедурами их обработки на протяжении всей логистической цепи;

ZAPP (експорт) – ZODIAK (імпорт) – для организации взаимодействия экспортеров, импортеров, таможенных агентов, поставщиков логистических услуг, круиз-агентов, операторов терминалов и пр.;

HABIS – для организации информационного взаимодействия морских перевозчиков с железнодорожным и автомобильным транспортом;

GEGIS – для информационной поддержки и обеспечения безаварийных перевозок опасных грузов.

Каждая из вышеприведенных систем имеет свои уязвимости и проблемы с точки зрения информационной безопасности.

При исследовании безопасности AIS, проведенном компанией Trend Micro в 2017 году, рассматривались два направления атаки: первый — на AIS-провайдеров, собирающих данные с AIS-шлюзов, установленных на побережьях для сбора информации AIS и далее для предоставления коммерческих и бесплатных сервисов в реальном времени (например, MarineTraffic). Второй тип атаки – на уровне радиопередачи, т.е. самого протокола AIS. Атака на протокол была проведена с использованием SDR (software-defined radio). Архитектура протокола была разработана достаточно давно, механизмы валидации отправителя и шифрование передаваемых данных не были предусмотрены, так как вероятность использования дорогого «железного» радиооборудования для компрометации технологии расценивалась как низкая. Исследование показало возможность следующих сценариев:

– изменение данных о судне, включая его местоположение, курс, информацию о грузе, скорость и имя;

– создание «кораблей-призраков», опознаваемых другими судами как настоящее судно, в любой локации мира;

– отправка ложной информации про погоду конкретным судам, чтобы заставить их изменить курс для обхода несуществующего шторма;

– активация ложных предупреждений о столкновении, что также может стать причиной автоматической корректировки курса судна;

– возможность сделать существующее судно «невидимым»;

– создание несуществующих поисково-спасательных вертолетов;

– фальсификация сигналов EPIRB, активирующих тревогу на находящихся поблизости судах;

– возможность проведения DoS-атаки на всю систему путем инициирования увеличения частоты передачи AIS-сообщений.

Кроме того, персонал судна может выключать свою AIS, становясь «невидимкой» (по данным CyberKeel, довольно распространенная практика для прохождения опасных участков акватории, таких как Аденский залив, «вотчину» сомалийских пиратов), а в некоторых случаях менять транслируемую информацию вручную.

Нанесение на AIS-карты несуществующего военного корабля страны А в территориальных водах страны Б может спровоцировать дипломатический конфликт. Кроме того, атака злоумышленника также может привести к отклонению судна с курса в результате подмены сообщений о возможном столкновении с ним или к «заманиванию» в определенную точку акватории путем создания ложного сигнала аварийного радиобуя.

В комплекте с ECDIS-системами обычно не поставляется никаких средств информационной защиты. Кроме того, Windows-системы, развернутые на судах, которые долго находятся в рейсах, далеко не всегда успевают получить даже критически важные обновления безопасности в разумные сроки. Уязвимости ECDIS в основном связаны с сервером Apache, устанавливаемым в комплексе с системой. Внедрить вредоносный код может как внешний нарушитель через Интернет, так и член команды через физический носитель, использующийся для обновления или дополнения навигационных карт. Имеющиеся уязвимости позволяли считывать, скачивать, перемещать, заменять и удалять любые файлы, находящиеся на рабочей станции. При таком развитии событий, атакующий получает доступ к чтению и изменению данных со всех сервисных устройств, подключенных к бортовой сети корабля.

Корректная работа ECDIS-системы очень важна, ее компрометация может привести к самым неблагоприятным последствиям — травмам и даже смертям людей, загрязнению окружающей среды и большим экономическим убыткам. «Замершее» судно, потеряв возможность корректной навигации, перекроет оживленный канал или шлюз на неопределенный срок, что вызовет при определенном стечении обстоятельств огромные экономические убытки. Танкер, перевозящий нефть или другие химические продукты и севший на мель из-за навигационных ошибок, — готовый сценарий экологической катастрофы.

Морская индустрия активно пользуется спутниковыми технологиями SATCOM (Satellite Communications) для доступа в Интернет, связи судно – судно и судно – суша, GPS/DGPS для определения местоположения и навигации, а также отслеживания перевозимых грузов. Исследование безопасности систем GPS-трекинга Globalstar, проведенное компанинй Synack, показало, что эксплуатация найденных уязвимостей приводит к перехвату и подмене информации или глуше-

нию сигнала. В сети Simplex, основанной на радиопередаче, используемой компанией Globalstar для передачи данных между трекерами, спутниками и наземными станциями, отсутствуют механизмы аутентификации и шифрования, обслуживающие работу систем, а механизм передачи данных, работающий только в одну сторону, не представляет возможности валидации переданных данных. Данная проблема присутствует не только в Globalstar.

Проверка, проведенная IO Active, терминалов спутниковой связи, используемых в судоходстве, выявила такие критические бреши в безопасности, как использование устройствами незащищенных или даже недокументированных протоколов, заведенные «фабрично» учетные записи, возможность эксплуатирования функции сброса пароля, бэкдоры.

Крайне показательный случай компрометации спутниковых систем произошел в июле 2013 года. Студенты из Техасского университета в Остине смогли отклонить от курса яхту стоимостью $80 млн, используя оборудование, цена которого не превышала $3 тыс. С помощью имитатора GPS-сигналов (используются, к примеру, при калибровке оборудования), дублируя сигнал настоящего спутника и постепенно повышая мощность, им удалось «убедить» навигационную систему судна принимать сообщения спуфингового устройства и отбрасывать сигнал настоящего спутника как помехи. После того как навигационная система начала ориентироваться по данным двух спутников и атакующего устройства, исследователям удалось отклонить судно от первоначального курса.

Международная морская организация (International Maritime Organization, IMO), учитывая сложившуюся в сфере информационной безопасности морской отрасли ситуацию, в 2017 году разработала и приняла ряд документов по кибербезопасности:

– Guidelines on maritime cyber risk management (FAL 41/17) – “Рекомендации по управлению киберрисками в морской отрасли» Комитета по упрощению формальностей (КУФ) [3]. Текущая версия документа FAL 45/22 принята 28.06.2021 [4];

– Maritime cyber risk management in safety management systems (MSC.428(98)) – Резолюция Комитета по морской безопасности (КМБ)

«Управление киберрисками в системах управления безопасностью морской отрасли» [5];

– Guidelines on maritime cyber risk management (MSC-FAL/Circ.3) – Циркуляр КМБ и КУФ «Рекомендации по управлению киберрисками в морской отрасли». Текущая версия документа MSC-FAL.1/Circ.3/Rev.1 принята 14.06.2021 [6];

– The guidelines on cyber security onboard ships (Version 2.0) – Рекомендации по кибербезопасности на судах, разработанные Baltic and International Maritime Council (BIMCO, Балтийский и международный морской совет). BIMCO – неправительственная организация, занимающаяся вопросами морской судоходной политики, унификации транспортных документов и информированием членов по различным аспектам международной морской торговли, которая функционирует с 1905 года и объединяет судовладельцев, судовых брокеров и агентов, клубы взаимного страхования и ассоциации из 121 страны мира. Текущая версия документа Version 4.0 принята в феврале 2021 [7].

Приложение № 10 Резолюции MSC.428(98) [5] настоятельно рекомендует администрациям обеспечить надлежащее рассмотрение киберрисков в системах управления безопасностью не позднее 1 января 2021 года.

В [6] отмечается, что кибертехнологии стали необходимыми для эксплуатации и управления множеством систем, важных для безопасности судоходства и защиты морской окружающей среды, однако уязвимости, создаваемые доступом, соединением или сетевым подключением этих систем, могут привести к киберугрозам, которые необходимо устранять. Рекомендации определяют морские киберугрозы как риски технологическому ресурсу со стороны потенциальных событий, которые могут привести к сбоям в перевозке грузов и пассажиров, безопасности мореплавания или безопасности судна, в связи с повреждением, утратой или компрометацией связанных с судоходством информации или систем.

Эти риски могут быть обусловлены уязвимостью, обусловленной неадекватной работой, интеграцией, обслуживанием и разработкой киберсистем, а также преднамеренными и непреднамеренными киберугрозами.

Угрозы представляют собой вредоносные действия (например, взлом или внедрение вредоносных программ) или непреднамеренные

последствия доброкачественных действий (например, обслуживание программного обеспечения или разрешения пользователя). Как правило, эти действия вызывают уязвимость (например, устаревшее программное обеспечение или неэффективные брандмауэры) или используют уязвимость в операционной или информационной технологии.

С точки зрения Рекомендаций [6] уязвимые судовые системы могут включать системы связи, обработки и управления грузом, управления двигателями, машинами и энергопитанием, контроля доступа, обслуживания и управления пассажирами; системы ходового мостика, административные системы и сети; публичные интернет-сети судна, предназначенные для использования пассажирами и другие системы:

Несмотря на то что необходимые подзаконные акты во исполнение Закона еще не изданы, к его требованиям необходимо отнестись со всей серьезностью уже сейчас.

Исходя из опыта реализации новых законов, в частности в сфере транспортной безопасности, можно прогнозировать, что вступление в силу Закона может повлечь увеличение бюрократических процедур, количества обязательных для субъекта транспортной инфраструктуры и/или транспортного средства документов, объема контрольных и надзорных мероприятий. Содержащиеся в Законе определения позволяют сделать предварительный вывод о том, что к критической информационной инфраструктуре транспорта может быть отнесен очень широкий круг объектов, включая судовые, береговые и портовые системы. Необходимо отметить, что эта проблема коснется всей транспортной сферы, а не только морского и речного транспорта.

Выводы

В данной работе определены наиболее распространенные информационно-коммуникационные системы, используемые в водно-транспортном комплексе, их особенности и уязвимости, и возможные последствия нарушения кибербезопасности в таких системах и перспективные пути нейтрализации уязвимостей.

Список литературы:

1. Cybersecurity in the Maritime Sector: ENISA Releases New Guidelines for Navigating Cyber Risk. [URL]:

https://www.enisa.europa.eu/news/enisa-news/cybersecurity-in-the-maritime-sector-enisa-releases- new-guidelines-for-navigating-cyber-risk

2. Maritime Ciber-Risks. [URL]: https://maritimecyprus.files.wordpress.com/2015/06/maritime-cyber-risks.pdf

3. Guidelines on maritime cyber risk management (FAL 41/17) [URL]: https://wwwcdn.imo.org/localresources/en/OurWork/Facilitation/Documents/FAL%2041-17.pdf

4. Guidelines on maritime cyber risk management (FAL 45/22) [URL]: https://imokorea.org/upfiles/board/21.%20FAL%2045%20%B0%E1%B0%FA%BA%B8%B0%ED%BC%AD%28%BF%B5%BE%EE%29%281%29.pdf

5. Maritime cyber risk management in safety management systems (MSC.428(98)) [URL]: https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/Resolution%20MSC.428(98).pdf

6. Guidelines on maritime cyber risk management (MSC-FAL.1/Circ.3/Rev.1) [URL]: https://wwwcdn.imo.org/localresources/en/OurWork/Facilitation/Facilitation/MSC-FAL.1-Circ.3-Rev.1.pdf

7. The guidelines on cyber security onboard ships (Version 4.0). [URL]: https://www.ics-shipping.org/wp-content/uploads/2021/02/2021-Cyber-Security-Guidelines.pdf

8. Boyes H., Isbell R., Luck A. Cyber Security for Portsand Port Systems. – London: Institution of Engineering and Technology, 2020. – 71 p.

9. Баронова О., Турти М., Мавроді В. Аналіз впливу загроз інформаційній безпеці на проблеми портової галузі // Матеріали 9-ої Міжнародної науково-технічної конференції «Інформаційні системи та технології ІСТ-2020». – Харків: ХНУРЕ, 2020. – С.279-282.

10. Блінцов В.С., Майданюк П.В. Концепція системи захисту інформації, що циркулює на об`єктах морської інфраструктури. Збірник наукових праць НУК. Миколаїв: НУК. 2016. № 1.

УДК 004.056.5;057.2

СРАВНИТЕЛЬНАЯ ХАРАКТЕРИСТИКА ПРОГРАММНЫХ КОМПЛЕКСОВ METASPLOIT И MAXPATROL 8

Автор: *Дзюбас Д.С., Национальный университет кораблестроения имени адмирала Макарова, г. Николаев, Украина*

Научный руководитель: *Турты М.В., к.т.н., доцент, Национальный университет кораблестроения имени адмирала Макарова, г. Николаев, Украина*

Применение сканеров уязвимостей позволяет решать различные задачи [1, 2]. Такие инструменты используют не только для самостоятельной проверки на наличие брешей в инфраструктуре предприятия. Функциональность сканера уязвимостей даёт, например, возможность провести инвентаризацию ИТ-ресурсов и определить, какие приложения и какой версии установлены на рабочих станциях и серверах. При этом сканер покажет, какое программное обеспечение имеет уязвимости, и предложит установить патч, обновить версию или остановить те или иные службы и отключить протоколы, если они представляют собой угрозу информационной безопасности. Если присутствуют ошибки в скриптах, это также будет обнаружено сканером.

На данный момент существуют различные сканеры уязвимостей, и, соответственно, для пользователя возникает задача выбора лучшего сканера для конкретных условий его функционирования.

Целью данной работы является объективная оценки двух программных комплексов по сканированию уязвимостей MetasPloit и MAXPATROL 8.

Для достижения поставленной цели необходимо провести анализ программ, определить критерии сравнения и степень их значимости.

MetasPloit framework создан для предоставления информации об уязвимостях, помощи в создании сигнатур для IDS, создания и тестирования эксплойтов, имеет псевдографический интерфейс.

В **Metasploit** входят различные виды библиотек, которые представляют собой набор задач, операций и функций, которые могут быть испо-

льзованы различными модулями системы. Самая фундаментальная часть framework написана на языке **Ruby Extension (Rex)**. Некоторые компоненты Rex включают подсистему сокетов (wrapper socket subsystem), реализацию клиентских и серверных протоколов, регистрацию подсистемы (logging subsystem), а также ряд других полезных классов.

Metasploit состоит из четырех пользовательских интерфейсов: msfconsole, msfcli, msfgui, msfweb.

Выбор эксплойта осуществляется после сбора достаточной информации о цели утилитой **Nmap**.

При выборе эксплойта используются такие команды как:

– **show payloads** и **show exploits –** показывают список доступных эксплойтов и payloads;

– **search exploit** – поиск конкретного эксплойта;

– **use exploit –** активация эксплойта.

Данная программа может быть полезна системным администраторам и специалистам по безопасности для защиты компьютерных систем. Для обычного же пользователя, стандартная (бесплатная) версия MetasPloit frameworks предоставляет существенно суженный спектр доступных, функций (большая часть будет закрыта, по причине, отсутствия лицензии), которые позволяют визуализировать все активные и скрытые процессы в операционной системе (ОС) пользователя, проверить порты на наличие открытых, также проверить их подводку к защитным системам ОС. Цена данного продукта варьируется от 50$ до 100$ за стандартную версию.

MaxPatrol 8 является продуктом корпоративного класса для крупных заказчиков с неограниченно большим количеством узлов в сетевой инфраструктуре и обладает широким спектром функций:

– проводит комплексный анализ на наличие уязвимостей в сложных системах, включая платформы Windows, Linux, Unix, сетевое оборудование Cisco, Juniper, Huawei, Check Point, системы виртуализации Hyper-V, VMware, веб-серверы Microsoft IIS, Apache HTTP Server, Nginx, серверы веб-приложений IBM WebSphere, Oracle WebLogic, Apache Tomcat, а также ERP-системы SAP и 1С;

– анализирует безопасность веб-приложений и позволяет обнаружить большинство уязвимостей в них: внедрение SQL-кода, межсайтовое выполнение сценариев (XSS), запуск произвольных программ;

– проверяет СУБД, такие как Microsoft SQL, Oracle, PostgreSQL, MySQL, MongoDB, Elastic;

– анализирует сетевые настройки, парольную политику, права и привилегии пользователей, позволяет управлять обновлениями.

Лицензии на Max Patrol 8 отличаются по функциональным возможностям:

– PenTest – поддержка тестирования на проникновение;

– PenTest & Audit – поддержка тестирования на проникновение и системных проверок;

– PenTest & Audit & Compliance – поддержка тестирования на проникновение, системных проверок и контроля соответствия стандартам отрасли.

Для того, чтобы запустить сканирование, нужно создать задачу, в параметрах которой нужно указать профиль сканирования. Например, выберем Fast Scan – простое сканирование портов, с определением версией сервиса, который слушает порт. В среднем процедура занимает 15-20 минут. На главной странице выводится общая информация об просканированном узле. Как показала экспериментальная проверка, MaxPatrol находит все уязвимости, присутствующие в проверяемой системе (их количество совпадает с числом, указанным в описании к дистрибутиву Metasploitable).

Интерфейс MaxPatrol 8 достаточно ясен, что позволяет при помощи стандартной версии провести стандартную сканерную проверку как и высококвалифицированному специалисту информационной защиты, так и обычному пользователю. Цена версии PenTest равна 65$, версии с более широкими возможностями имеют большую цену.

Выводы

В результете проведенного анализа двух программ для тестирования уязвимостей ОС, MetasPloit Frameworks и MaxPatrol 8, в качестве критериев сравнения были выбраны: операции с уязвимостями, конечный пользователь, качество интерфейса и ценовой диапазон. Сравнение MetasPloit Frameworks и MaxPatrol 8 позволяет сделать следующие выводы:

1. MetasPloit – программа, которая ориентирована на обнаружение-исправление уязвимостей ОС и рассчитана на специалиста, который вы-

полняет определённые задачи. Обычный пользователь может использовать эту программу для своих целей, но это может вызвать определённые трудности. Первая из которых – это полностью текстовый интерфейс, который сложен для неподготовленного пользователя. Вторая – это поддержка только английского языка. Третья – это ценовой вопрос.

2. MaxPatrol 8 – программа, которая ориентирована на защиту-обнаружение уязвимостей, позволяет проводить комплексное сканирование в сложных системах и рассчитана на корпорацию, а не на одиночного пользователя. Однако, это не исключает возможности её использования для проверки обычного ПК. В отличие от MetasPloit'a, это программа имеет дружественный интерфейс, поддерживает большое количество языков (более 50 языков) и в целом направлена на широкомасштабное распространение данного продукта. Стоимость минимальной версии MaxPatrol примерно на 30% превышает стоимость минимальной версии MetasPloi.

Список литературы:

1. Официальный сайт Rapid7. MetasPloit Frameworks. URL: https://www.metasploit.com/

2. Официальный сайт PtsSECURITY. MaxPatrol 8, URL: https://www.ptsecurity.com/ru-ru/products /mp8/

УДК 004.056.5;057.2

ГРАФИ ТА ШТУЧНИЙ ІНТЕЛЕКТ В СИСТЕМАХ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

Автор: *Манько С.В., Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

Науковий керівник: *Турти М.В., к.т.н., доцент, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

Тенденцією розвитку сучасних інформаційні технології обробки і захисту інформації є активне впровадження засобів штучного інтелекту, внаслідок чого з'являються нові математичні моделі об'єктів і процесів комп'ютеризації, а традиційні моделі набувають нового змісту.

Метою даної роботи є визначення перспектив застосування графів і систем штучного інтелекту в системах технічного захисту інформації.

Для досягнення поставленої мети необхідно вирішити наступні задачі:

– провести аналіз типів графів, методів їх математичного опису та графічного відображення;

– визначити типові задачі, які розв'язуються за допомогою графів;

– визначити галузі застосування графів в інформаційній безпеці;

– визначити перспективні напрями сумісного застосування графів і систем штучного інтелекту в системах технічного захисту інформації.

Теорія графів– розділ математики, особливістю якого є геометричний підхід до вивчення об'єктів. Граф можна розглядати як об'єкт, що складається з двох множин – множини точок (вершин, вузлів) X і множини ліній (ребер) U, які з'єднують вершини. Кожне ребро відповідає невпорядкованій парі вершин з множини X.

Математичний опис графа включає позначення множин вершин і ребер, наприклад, $G=(X, U)$. Елементи множин X і U можуть містити індекси, які для вершин позначають їх номери, а для ребер позначають номери вершин, які з'єднуються ними.

Ребрам може приписуватися властивість відношення (наприклад, довжина дороги, відстань, ціна, прибуток, пропускна здатність, швидкість, ступінь ризику, ймовірність деякої дії, взаємна приязнь, тощо). Числа, які приписані ребрам, називаються довжиною ребра (ціною, вагою).

Розмітка графів – позначення вершин і/або ребер графа.Вершини графа можуть позначатись літерами, цифрами, кружечками, точками або іншими символами.

Існують різні типи графів: кінцевий граф, нуль–граф, порожній граф, орієнтований граф (орграф), неорієнтований граф (неорграф), змішаний граф, мультиграф, повний (повнозв'язаний) граф, щільний граф, симетричний граф, ізоморфні графи, плаский граф, планарний граф, багаторівневий граф, мережний граф, однорідний граф ступеня *t,* багатокольоровийі граф, дводольний граф (біграф, двочастковий граф), зв'язний граф, незв'язний граф, дерево, зв'язний граф без циклів, двійкове (бінарне) дерево, повне (закінчене) двійкове дерево, неповне

(не суворе) бінарне дерево, Б-дерево, ідеальне двійкове дерево, збалансоване дерево, ідеально збалансоване дерево (за Адельсон-Вельським та Ландісом, AVL–збалансоване бінарне дерево), червоно-чорне дерево.

Графи можуть бути представлені у вигляді графічних зображень, матриць (математичних описів, наприклад, матриця суміжності, матриця інцидентності, матриця шляхів), зв'язаних списків в певному середовизі програмування. Зображення, наприклад, мережі у вигляді графа має лише наочне значення для пояснень і контролю при виконанні ручних операцій, а складний аналіз на комп'ютері відбувається з матрицями. Тому виявлення особливостей вигляду матриць та їх використання для кожної логічної задачі має не менше практичне значення ніж виявлення особливостей графів.

Типові задачі, які розв'язуються на графах: впорядкування вершин графу; відтинання піддерев, кущів, гілок, вузлів графа, які задовольняють/не задовольняють певним вимогам; визначення максимального/мінімального потоку в орієнтованому і неорієнтованому графі; визначення найкоротшого/найдовшого шляху в орієнтованій і неорієнтованій мережі; вихід з лабіринту; проходження дерев; задача комівояжера.

На деревах можуть бути реалізовані різноманітні алгоритми обробки даних, найбільш розповсюдженими з яких і широко використовуваними при реалізації алгоритмів захисту інформації є: сортування з проходженням бінарного дерева; сортування методом турніру з вибуванням; стискання інформації; подання виразів за допомогою дерев; представлення ієрархічної структури каталогів файлової системи.

Графи широко використовуються при моделюванні систем. Будь-яка організована сукупність об'єктів (система управління державою та підприємством, ринок, системи захисту інформації) може бути представлена у вигляді графу. Моделі більшості задач, пов'язаних із пошуком рішення в просторі станів, мають мережний характер.

Графи можуть застосовуватися при розв'язку задач математичного програмування, зокрема бінарні дерева можуть застосовуватися при розв'язку задач цілочискльного програмування, а мережкві графи – при розв'язку задач динамічного програмування щодо переведення системи з поточного стану у новий заданий стан.

При аналізі надійності систем використовується дерево відмов, яке є одним із видів дерева наслідків, що є окремим випадком дерева цілей. Термін «дерево цілей» використовується для деревоподібних ієрархічних структур і в залежності від мети досліджень має не тільки різне змістовне навантаження вузлів і ребер, а й різні назви: дерево рішень, дерево цілей і функцій, дерево проблем, дерево напрямків розвитку (дерево прогнозування розвитку, прогнозний граф), дерево відмов (дерево наслідків). Дерево відмов наочно відображає можливу послідовність відмов обладнання або реалізації загроз в інформаційній системі з вказаними ймовірностями відмов. Листям таких дерев є елементи досліджуваної системи. За деревами відмов визначають ймовірності відмов елементів, підсистем і системи в цілому, ймовірність працездатності системи, найбільш критичні вузли з точки зору відмовостійкості підсистем і системи в цілому.

Когнітивна карта (знаковий граф, карта пізнання) у вигляді орієнтованого графу відображає суб'єктивне сприйняття особою або групою осіб певної предметної галузі (складного об'єкта, проблеми, функціональної системи), і призначена для виявлення і усвідомлення узагальнених закономірностей причинно-наслідкових (казуальних) зв'язків в цій галузі. Когнітивна карта містить елементи двох типів вузли- концепти та казуальні зв'язки, представлені дугами з розміткою у вигляді знаків, базовими з яких є «+» (прямий зв'язок, два концепти змінюються в одному напрямі), «-» (зворотний зв'язок, зв'язані концепти змінюються в протилежних напрямах), «0» (зв'язок між концептами відсутній).

Для аналізу процесів в системах масового обслуговування (СМО), які часто використовуються як моделі телекомунікаційних систем, використовуються орієнтовані графи переходів між дискретними станами системи, де вершинами графу є стани S_i, що мають ймовірність P_i, а можливі переходи у стани S_{i-1} та S_{i+1} відображують направленими дугами, вага яких дорівнює добуткам відповідних інтенсивностей потоків подій і ймовірностей знаходження системи у відповідному стані. Класичним застосуванням методів теорії СМО є аналіз систем, в яких наявні черги і вирішуються питання із обслуговування ряду (потоку)

вимог (заявок на обслуговування) від людей, приладів, подій. Будь-який апаратно-програмний комплекс може розглядатися як обслуговуючий прилад по відношенню до *n* операторів, а засоби захисту інформації – як пункти обслуговування загроз, яким вони протидіють.

При побудові моделей дискретно-подібних систем, в яких відбувається стрибкоподібна зміна станів, для моделювання асинхронних інформаційних потоків використовується мережа Петрі, яка графічно відображається дводольним орієнтованим мультиграфом:

Класичним застосуванням мереж Петрі є аналіз функціонування систем, в результаті якого визначаються живучість системи, наявність тупикових станів, наявність циклів тощо.

Широкі можливості аналізу систем надають різновиди мереж Петрі: мережі Петрі із змінною кратністю дуг, кольорові (розфарбовані) мережі Петрі, мережі подій, *E*-мережі, мережі Петрі із затримками в часі, нечіткі мережі Петрі.

В галузі інформаційної безпеки та інформаційних технологій відомі роботи науковців і практиків, які розв'язують за допомогою мереж Петрі наступні задачі:

1. Моделювання процесів обчислення результатів математичних операцій і представлення складних алгоритмів обчислень на основі моделі «чорної скрині».

2. Обробка текстової інформації, машинний синтезу зв'язних текстів.

3. Інтеграція знань у системах автоматизованого проектування технологічних процесів. Для динамічного опису виробу та процесів його виготовлення у таких системах може використовуватися інкрементаційний метод із використанням високорівневих мереж Петрі для інтеграції знань, поданих у вигляді продукційних правил і фреймів.

4. Апробація методик підготовки персоналу до оперативного управління в умовах надзвичайних ситуацій.

5. Аналіз та створення Grid-систем. Імітаційна модель функціонування вузла Grid-системи і взаємодії вузлів при роботі із спільною пам'яттю з урахуванням черги на використання спільних ресурсів на основі мереж Петрі дозволяє забезпечити синхронізацію доступу до спільних ресурсів (даних) Grid-системи при виконанні паралельних обчислень. Аналіз побудованої моделі дозволяє визначити наявність у

Grid-системи необхідних для забезпечення коректної синхронізації доступу до даних і відсутність блокувань властивостей мереж Петрі – живості мережі, обмеженості мережі та досяжності всіх її позиції.

6. Захист програмних продуктів. Метод захисту полягає в тому, що до програми додається захисний фрагмент коду, що реалізує запуск спеціально розробленої мережі Петрі у якій переходи мають пріоритети. Мережа складається із блоків, кожний з яких містить кілька позицій для завдання початкового маркуванняμ, їх кількість *n* дорівнює кількості бітів у ключі. Перед запуском мережі в них записується уведений користувачем ключ. При такому підході злом захисту стає недоцільним, тому що швидкість обчислень при програмній емуляції знижується.

7. Побудова персоналізованих флеш-накопичувачів даних з апаратним захистом інформації на основі формалізації процесів автентифікації користувачів флеш-накопичувачів мережами Петрі

8. Інтеграція компонентів захисту мережного периметру.

9. Проектування систем управління інформаційною безпекою.

10. Моделювання процесів управління ризиками інформаційної безпеки за допомого. розфарбованих мереж Петрі, розфарбованих мереж Петрі і гіперграфів. В останньому випадку множину вершин W гіперграфу складають ідентифіковані активи організації. Множину ребер формують за наступним принципом: у випадку, якщо від функціонування активу не залежить функціонування інших активів, то ребро включає виключно вершину з нанесеним активом; у випадку, якщо від функціонування активу залежить функціонування інших активів, то ребро включає вершину з нанесеним активом та вершини із всіма залежними активами. Сформовані ребра гіперграфу H у мережі Петрі виступають у якості позицій «актив».

11. Оцінювання живучості систем захисту інформації корпоративних мереж зв'язку шляхом дослідження моделі на мережі Петрі.

12. Моделювання системи контролю доступу на основі нечітких часових мереж Петрі з інгібіторними зв'язками.

13. Моделювання системи безпеки. Ухвалення рішень з коректування безвихідних і небажаних ситуацій і при ідентифікації функціо-

нальних порушень систем може здійснюватися після перевірки їх ефективності на математичній моделі. При цьому можуть використовуватися всі моделі, засновані на теорії графів: когнітивні моделі, мережі Петрі, ланцюги Маркова, системи масового обслуговування (СМО), алгоритми, імітаційні моделі, потокові оптимізаційні моделі, семантичні мережі експертних систем (ЕС), нейронні мережі (наприклад, персептрони), кінцеві і клітинні автомати, фрактали.

Висновки

В даній роботі проведено аналіз аналіз типів графів, методів їх математичного опису та графічного відображення; визначені типові задачі, які розв'язуються за допомогою графів, галузі застосування графів в інформаційній безпеці і перспективні напрями сумісного застосування графів і систем штучного інтелекту в системах технічного захисту інформації.

В разі необхідності побудови моделей для аналізу й ухвалення рішень в умовах хаосу, невизначеності, протидії, конкуренції, конфліктів і кооперації виникає потреба застосування складних графоаналітичних моделей з багатьма динамічними, стохастичними, нечіткими, нелінійними і багатовимірними чинниками,. Саме таким вимогам відповідають динамічні моделі на мережах Петрі та імітаційні моделі. Імітаційні моделі легко інтегрують у себе всі можливі види інших моделей, а прості мережі Петрі можуть бути легко ускладнені до так званих "кольорових", "часових", "вірогідних", "функціональних", "ієрархічних" та інших видів мереж Петрі. Існують однозначні правила взаємного перетворення алгоритмів і мереж Петрі, що дозволяє легко переходити з імітаційної моделі й алгоритму в мережу Петрі і назад; алгоритми перетворення мережевих графіків і когнітивних карт у мережі Петрі.

Список літератури:

1. Математика в программировании. URL: https://unetway.com/blog/matematika-v-programmirovanii#:~:text=%D0%92%D0%BE%2D%D0%BF%D0%B5

2. Кузьменко І.М. Теорія графів. [Електронний ресурс]: навч. посіб. – Київ: КПІ ім. Ігоря Сікорського, 2020. – 71 с. URL: https://ela.kpi.ua/bitstream/123456789/35854/1/Teoriia_hrafiv.pdf

УДК 004.056.05

АКТУАЛЬНІ ПИТАННЯ ЗАХИСТУ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ МЕРЕЖАХ

Автор: *Садалюк Є.О., студент, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

Науковий керівник: *Турти М.В., к.т.н., доцент, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

Масове застосування персональних комп'ютерів, на жаль, виявилося пов'язаним з появою самовідтворюваних програм-вірусів, що перешкоджають нормальній роботі комп'ютера, руйнують файлову структуру дисків і завдають шкоди збереженої в комп'ютері інформації. Проникнувши в один комп'ютер, комп'ютерний вірус здатний поширитися на інші комп'ютери.

Для виявлення, видалення і захисту від комп'ютерних вірусів розроблено багато видів спеціальних програм, які дозволяють виявляти і знищувати віруси – антивірусів.

Метою даної роботи є проведення порівняльного аналізу ефективності антивірусників AvastFree та AVG на основі теоретичних та експериментальних даних.

Антивірус Avast має дружній, нескладні і зрозумілі засоби настроювання доступу до всіх параметрів захисту. Avast забезпечує високий рівень виявлення всіляких комп'ютерних загроз, в тому числі вірусів, шпигунів, інтернет-хробаків. Він має вбудований антишпигунський модуль і здатен виявляти загрози у вигляді руткітів, оскільки має вбудований антируткіт.

Avast Free Antivirus постійно моніторить систему в режимі реального часу, скануючи файли, що запускаються і процеси. Для забезпечення міцного захисту має сенс періодично запускати наявний звичайний сканер з повною перевіркою файлової системи і можливістю перевірки в середині архівів. Крім того, антивірус добре захищає і власні модулі.

Avast Free Antivirus перевіряє на наявність шкідливого коду, перехоплюючи попередньо всю вхідну і вихідну поштову кореспонденцію, а також повідомлення інтернет пейджерів і файли, поширювані за технологією P2P. За допомогою Web-екрану він захищає користувача від небажаних сайтів, що поширюють віруси і заражені скрипти, тобто є мережевий екран.

Нова технологія Cyber Capture є хмарним файловим сканером для невідомих загроз. Виявлені підозрілі файли Avast спочатку поміщає в безпечну ізольовану зону і миттєво передає в лабораторію Avast, де проводиться ретельний аналіз і ідентифікація загрози. Такому аналізу піддаються невідомі запщені файли, викачані з Інтернету, як правило ті, які мають статус підозрілих, тобто не наявні в базах, але чиї дії визначаються антивірусом як схожі з поведінкою деяких вірусів. Avast виробляє "хмарні" оновлення в реальному часі використовуючи технологію потокової передачі. Про різні події (оновлення, виявлення загроз тощо) антивірус інформує користувача спливаючими вікнами. Він також автоматично виявляє вразливості домашньої мережі Wi-Fi і наявності несанкціонованих підключень до неї.

Режим «Не турбувати» блокує відволікаючі увагу спливаючі повідомлення під час гри, перегляду фільму або презентації в повноекранному режимі.

Avast Free Antivirus отримав позитивні відгуки користувачів щодо пошуку і лікування операційної системи від черв'яків. Правда, як показала експериментальна перевірка, під час сканування він практично не дозволяє працювати за комп'ютером – процесор буде завантажений перевіркою. Напевно, зараз це єдиний вагомий мінус цтого антивіруса.

Розробники забезпечили AVG Anti-VirusFreeEdition хорошим антивірусним монітором – ResidentShield, який у фоновому режимі сканує всі файли, що потрапляють на комп'ютер, забезпечуючи постійний антивірусний захист. Anti-Virus відповідає за виявлення вірусів, а компонент Anti-Spyware захищає від шпигунських програм, наприклад таких, які таємно збирають персональні дані з комп'ютера користувача. Крім того, є і спеціальний модуль IdentityProtection, який запобігає перехопленню або крадіжці логінів і паролів користувачів. Ці компоненти мають потребу в регулярному оновленні та не мають на-

лаштувань. Блок Anti-Rootkit займається пошуком шкідливого програмного забезпечення, прихованого в операційній системі.

Унікальна функція AVG Anti-VirusFreeEdition – SocialNetworkingProtection, вперше реалізована саме в антивирусах AVG, – захищає при роботі в соціальних мережах, як то «Вконтакте» або Facebook. Модуль сканує файли і повідомлення, що передаються по соціальній мережі, і може вчасно визначити спробу «підробки» сторінки популярного сервісу, що зараз є поширеним способом шахрайства.

Корисним є наявне в цьому антивірусі «Сховище вірусів», яке дозволяє відновити файл при помилковому спрацьовуванні. Крім того, звідси можна також відправляти файли на аналіз в антивірусну лабораторію.

Додатковий компонент AVG PC Analyzer допомагає виявляти різні проблеми в реєстрі комп'ютера. Він сканує комп'ютер і виявляє певні проблеми, для виправлення котрих треба буде завантажити AVG PC Tuneup. Це набір програм для оптимізації системи та усунення в першу чергу тих проблем, які виникли в результаті дії вірусів. Він також дозволяє видаляти непотрібні файли і виявляти помилки в файловій системі. Утиліта йде як додаток до антивірусу і, на відміну від останнього, не є вільнорозповсюджуваною, але один раз нею можна скористатися безкоштовно.

Висновок

Проведений порівняльний аналіз AvastFree та AVG Anti-VirusFreeEdition на основі теоретичних та експериментальних даних показав, що ефективність AVG Anti-VirusFreeEdition в повній мірі відповідає заявленій розробником, у відмінності від AvastFree.

Список літератури:

1. Безруков Н.Н. Классификация компьютерных вирусов и методы защиты от них. URL: http://www.viruslist.com
2. Михайлов А.В. Компьютерные вирусы и борьба с ними. URL: http://prontocom.ru
3. Моисеенков И. Безопасность компьютерных систем. URL:http://journal-shkolniku.ru.

4. Мостовой Д.Ю. Современные технологии борьбы с вирусами. URL: http://www.academ.org

5. AvastFree Antivirus. URL:https://www.avast.ua/ru-ua/free-antivirus-download#pc

6. AVG. Бесплатный антивирус, который вы искали. URL: https://www.avg.com/ru-ru/homepage#pc

УДК 004.056.05

ЗАСОБИ МОДЕЛЮВАННЯ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ

Автор: *Садалюк Є.О., студент, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

Науковий керівник: *Турти М.В., к.т.н., доцент, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

При проектуванні комп'ютерних мереж вирішуються задачі аналізу інформаційних потоків, розробляється структура системи, обираються або розробляються методи і засоби захисту інформації, обирається обладнання, яке реалізує процедури обробки інформації та її захисту. Для оцінювання працездатності створюваної системи найчастіше використовується імітаційне моделювання.

Для моделювання процесу роботи мереж існує ряд програмних продуктів, які різняться як за умовами розповсюдження, так і за своїми функціональними можливостями []. Відповідно виникає задача оптимального вибору середовища дослідження властивостей певної комп'ютерної мережі.

Метою даної роботи є порівняльний аналіз сучасних засобів моделювання інформаційно-телекомунікаційних систем (ІТКС).

Для досягнення поставленої мети необхідно вирішити наступні задачі:

– визначити критерії оцінювання сучасних засобів моделювання ІТКС;

– оцінити сучасні засоби моделювання ІТКС за визначеними критеріями.

Існують спеціальні, орієнтовані на моделювання обчислювальних мереж, програмні системи, в яких процес створення моделі спроще-

ний. Такі програмні системи самі генерують модель мережі на основі вихідних даних про її топологію і використовувані протоколи, про інтенсивності потоків запитів між комп'ютерами мережі, протяжності ліній зв'язку, про типи використовуваного обладнання та програм. Програмні системи моделювання можуть бути вузько спеціалізованими і універсальними, що дозволяють імітувати мережі самих різних типів. Якість результатів моделювання в значній мірі залежить від точності вихідних даних про мережу, переданих в систему імітаційного моделювання.

Програмні системи моделювання мереж – інструмент, який може стати в нагоді будь-якому адміністратору корпоративної мережі, особливо при проектуванні нової мережі або внесення кардинальних змін у вже існуючу. Продукти цієї категорії дозволяють перевірити наслідки впровадження тих чи інших рішень ще до оплати придбаного обладнання. Звичайно, більшість з цих програмних пакетів коштують досить дорого, але й можлива економія може бути також дуже істотною.

Програми імітаційного моделювання мережі використовують у своїй роботі інформацію про просторове розташування мережі, кількість вузлів, конфігурацію зв'язків, швидкості передачі даних, використовувані протоколи і типи обладнання, а також про виконувані в мережі додатки. Зазвичай імітаційна модель будується не з нуля. Існують готові імітаційні моделі основних елементів мереж: найбільш поширених типів маршрутизаторів, каналів зв'язку, методів доступу, протоколів і т.ін. Ці моделі окремих елементів мережі створюються на підставі різних даних: результатів тестових випробувань реальних пристроїв, аналізу принципів їх роботи, аналітичних співвідношень. У результаті створюється бібліотека типових елементів мережі, які можна настроювати за допомогою заздалегідь передбачених у моделях параметрів.

Системи імітаційного моделювання зазвичай включають також набір засобів для підготовки вихідних даних про досліджувану мережу – попередню обробку даних про топологію мережі і визначення параметрів трафіку в моделі. Ці засоби можуть бути корисні, якщо мережа, що моделюється, являє собою варіант існуючої мережі і є можливість провести в ній вимірювання трафіку та інших параметрів,

потрібних для моделювання. Крім того, система комплектується засобами для статистичної обробки отриманих результатів моделювання.

Систем динамічного моделювання обчислювальної системи досить багато, вони розробляються в різних країнах. Аналіз літературних джерел в ході дипломного проектування дозволив виявити такі системи, вироблені в Румунії та інших країнах, які не є лідерами комп'ютерно-інформаційної індустрії.

Часто розвинуті системи діагностування встановленої обчислювальної системи (інтелектуальні кабельні тестери, сканери, аналізатори протоколів) також зараховують до систем моделювання, що не відповідає дійсності.

Класифікуємо системи по двох пов'язаних критеріями: ціна і функціональні можливості. Як і слід було очікувати, функціональні можливості систем моделювання жорстко пов'язані з їхньою ціною. Аналіз пропонованих на ринку систем показує, що динамічне моделювання обчислювальних систем – справа дуже дорога. Всі системи динамічного моделювання можуть бути розбиті на дві цінові категорії: дешеві (сотні і тисячі доларів) і high-end (десятки тисяч доларів, у повному варіанті – сто і більше тисяч доларів).

На жаль, знайти системи середнього цінового діапазону не вдалося, проте багато з них представляють собою набір пакетів і розкид у ціні однієї і тієї ж системи визначається комплектом поставки, тобто обсягом виконуваних функцій. Дешеві системи відрізняються від дорогих тим, наскільки докладно вдається в них описати характеристики окремих частин, що моделюються. Вони дозволяють отримати лише "приблизні" результати, не дають статистичних характеристик і не надають можливості проведення детального аналізу системи. Системи класу high-end дозволяють збирати вичерпну статистику по кожному з компонентів мережі при передачі даних по каналах зв'язку і проводити статистичну оцінку отриманих результатів. За функціональністю системи моделювання, що використовуються при дослідженні обчислювальних систем, можуть бути розбиті на два основні класи: системи, що моделюють окремі елементи (компоненти) системи і системи, що моделюють обчислювальну систему цілком.

У наступній таблиці наведені характеристики декількох популярних систем імітаційного моделювання різного класу – від простих

програм, призначених для установки на ПК, до потужних систем, що включають бібліотеки більшості наявних на ринку комунікаційних пристроїв і які у значній мірі автоматизувати дослідження мережі, що підлягає аналізу.

Таблиця 1 – Функціонально-вартісна оцінка програм для моделювання ІТКС

Компанія і продукт	Вартість ($)	Тип мережі	Необхідні ресурси	Примітки
American-HYTech, **Prophesy**	1495	ЛМ	8 Мб – ОП, 6 Мб - диск, DOS, OS/2, Windows	Оцінювання продуктивності при роботі з текстовими і графічними даними по окремих сегментах і мережі в цілому
CACI Product, **COMNET III**	34500-39500	ЛМ, ГМ	32 Мб – ОП, 100 Мб диск, Windows, Windows NT, OS/2, Unix	Моделює мережі X.25, ATM, FrameRelay, зв'язки LAN – WAN, SNA, DECnet, протоколи OSPF, RIP. Доступ CSMA/CD і FDDI та ін. Вбудована бібліотека маршрутизаторів 3COM, Cisco, DEC, HP, Wellfleat
MakeSystem, **NetMaker XA**	Від 6995	ЛМ, ГМ	128 Мб ОП, 2000 Мб диск, AIX, Sun OS, Sun-Solaris	Перевірка даних про топологію мережі; імпорт інформації про трафік, що отримується в реальному часі

Компанія і продукт	Вартість ($)	Тип мережі	Необхідні ресурси	Примітки
NetMagicSystem, **StressMagik**	2995	ЛМ	2 Мб ОП, 8 МБ диск, Windows	Підтримка стандартних тестів виміру продуктивності; імітація пікового навантаження на файл-сервер
NetworkDesignandAnalysisGroup, **AutoNet/ Designer**	25000	ГМ	8 Мб ОП, 40 Мб диск, Windows, OS/2	Визначення оптимального розташування концентратора в ГС, можливість оцінки економії коштів за рахунок зниження тарифної плати, зміни постачальника послуг і оновлення устаткування; порівняння варіантів зв'язку через найближчу і оптимальну точку доступу, а також через міст і місцеву телефонну мережу
NetworkDesignandAnalysisGroup, **AutoNet/ MeshNET**	30000	ГМ	8 Мб ОП, 40 Мб диск, Windows, OS/2	Моделювання смуги пропускання і оптимізація витрат на організацію ГС шляхом імітації пошкоджених ліній, підтримка тарифної сітки компаній AT & T, Sprint, WiTel, Bell
NetworkDesignandAnalysisGroup, **AutoNet/ Performance – 1**	4000	ГМ	8 Мб ОП, 1 Мб диск, Windows, OS/2	Моделювання продуктивності ієрархічних мереж шляхом аналізу чутливості до тривалості затримки, часу відповіді,

Компанія і продукт	Вартість ($)	Тип мережі	Необхідні ресурси	Примітки
				а також вузьких місць в структурі мережі
NetworkDesignandAnalysisGroup, **AutoNet/ Performance – 3**	6000	ГМ	8 Мб ОП, 3 Мб диск, Windows, OS/2	Моделювання продуктивності багатопротокольних об'єднань локальних і глобальних мереж; оцінювання затримок в чергах, прогнозування часу відповіді, а також вузьких місць в структурі мережі; облік реальних даних про трафік, що поступають від мережевих аналізаторів
System&Networks, **BONES**	20000-40000	ЛМ, ГМ	32 Мб ОП, 80 Мб диск, Sun OS, HP–UX, SunSolaris	Аналіз дії застосувань клієнт-сервер і нових технологій на роботу мережі
MIL3, **Opnet**	16000-40000		16 Мб ОП, 100 Мб диск, DEC AXP, Sun OS, HP-UX SunSolaris,	Має бібліотеку різних мережевих пристроїв, підтримує анімацію, генерує карту мережі, моделює смугу пропускання.

Висновки

Систем динамічного моделювання ІТКС досить багато. Програмні системи моделювання можуть бути вузько спеціалізованими і універсальними, що дозволяють імітувати мережі різних типів і можуть стати в нагоді при проектуванні і адмініструванні ІТКС. В даній роботі проведене оцінювання сучасних засобів моделювання ІТКС за критеріями вартості, вимог до ресурсів і спектру функцій.

Список літератури:

1. Моделирование сетей и систем связи, Учебное пособие – https://siblec.ru/ telekommunikatsii/modelirovanie-setej-i-sistem-svyazi#7

УДК 004.056.5; 004.89; 514.743.4

ТЕНЗОРЫ И ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В СИСТЕМАХ ЗАЩИТЫ ИНФОРМАЦИИ

Автор: *Стефанюк Ю.О., Национальный университет кораблестроения имени адмирала Макарова, г. Николаев, Украина*

Научный руководитель: *Турты М.В., к.т.н., доцент, Национальный университет кораблестроения имени адмирала Макарова, г. Николаев, Украина*

Динамика информационных технологий обуславливает периодическое возникновение решений, которые кардинальным образом изменяют сосотояние зашищенности объектов информационной деятельности как с точки зрения злоумышленников, так и с точки зрения службы защиты информации. В 2018 году было доказано [1], что на основе общедоступных данных нейронные сети, в которых реализуется адаптивный алгоритм обучения, могут определять индикаторы атак определенного типа, например, прямой атаки подбора пароля. Нейронные сети могут использоваться не только как типичные системы управления техническими средствами, а и для прогнозирования состояния объекта защиты, для построения защитных ботов и пр. [2].

Целью данной работы является определение перспектив применения тензоров и систем искусственного интеллекта в системах технической защиты информации.

Для достижения поставленной цели необходимо решить следующие задачи:

– проанализировать принципы функционирования нейронных сетей;

– проанализировать принципы формирования тензоров;

– определить основные области применения тензоров и систем искусственного интеллекта в системах технической защиты информации.

Искусственный интеллект (ИИ) – представляет собой систему или машину, которая способна анализировать входные данные и имитировать поведение человека на основе этих данных.

Яркими примерами действующих ИИ являются:

– Алиса – голосовой помощник, созданный компанией Яндекс.

– Сири – голосовой помощник, созданный компанией Apple.

– Автопилот созданный компанией Tesla.

Системы ИИ могут быть реализованы на основе нейронных сетей. Идеи простейших нейронных сетей, и их алгоритмы работы были разработаны еще в 1950 – 1970-х годах.

Искусственным нейроном (рис. 1) называют математическую модель человеческого нейрона. Нейрон представляет собой объект с несколькими входами и одним выходом. Входы имеют собственный, так называемый “вес” – числовое значение которое показывает насколько соответствующий вход влияет на состояние нейрона.

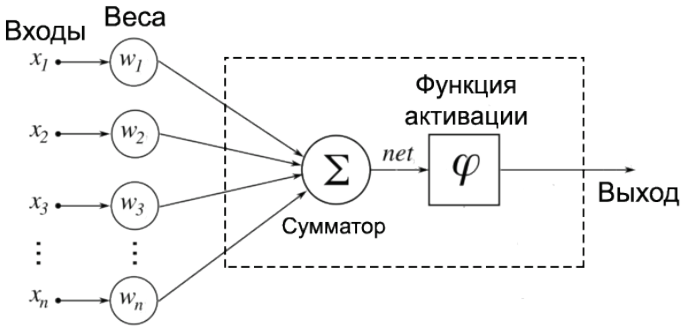


Рисунок 1 – Искусственный нейрон

Искусственный нейрон работает по такому алгоритму:

1. На входные каналы нейрона приходят значения;

2. Входные значения умножаются на веса – "взвешиваются".

3. Взвешенные входы суммируются в ячейке нейрона (на рис. 1 – изображено пунктиром)

4. К полученной сумме добавляется значение порога и преобразуется с помощью активационной (передаточной функции)

5. Полученное значение передается на выход.

Работу искусственного нейрона можно описать формулами:

$$S = \sum_{i=1}^{n} w_i x_i + b ;$$

$$Y = f(S),$$

где n – количество входов нейрона;

w_i – вес i-го входа нейрона;

x_i – значение, поступающее на i-го вход;

b – постоянное смещение, которое подается на сумматор по входу с весом 1;

Y – выходное значение нейрона,

$f(S)$ – активационная функция.

При работе с большими объемами данных в нейронных сетях применяются тензоры (рис. 2). Тензоры используются для анализа, транспортировки и хранения данных. Тензор имеет несколько определений:

1. Тензор – математический объект, не изменяющийся при изменении системы координат, представленный набором своих компонент и правилом преобразования компонент при смене базиса.

2. Тензор – это многомерный массив чисел. Обычно в нём больше двух измерений, так что он может быть изображён как многомерная сетка, состоящая из чисел.

В нейронных сетях тензоры используются в соответствии со вторым определением, то есть как многомерные массивы данных. Так, очень удобно, при написании нейронных сетей, состоящих из нескольких нейронов или слоев нейронов (рис. 3), объединять все входы – создавая таким образом тензор входных данных, веса этих входов – в тензоры весов.

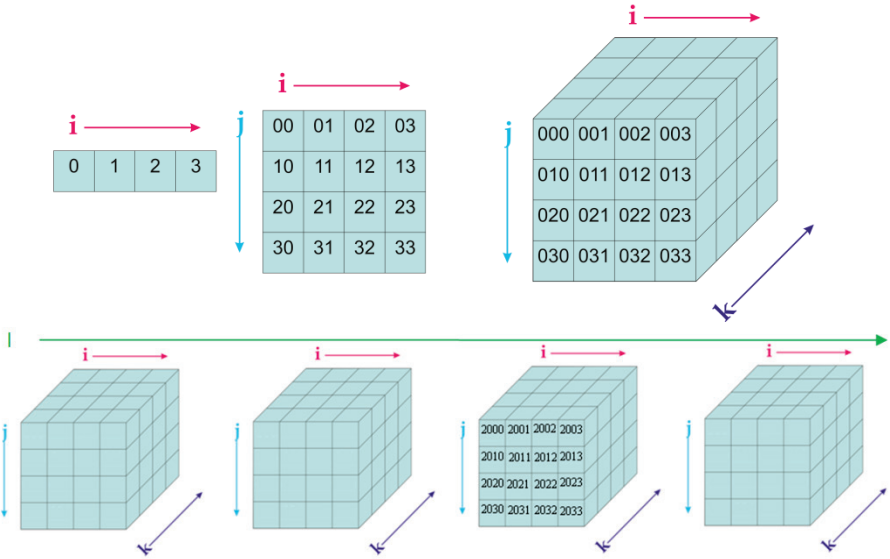


Рисунок 2 – Примеры тензоров разных видов

Выводы

В данной работе проведен анализ принципов функционирования нейронных сетей и принципов формирования тензоров, определены основные области применения тензоров и систем искусственного интеллекта в системах технической защиты информации.

Тензоры различных типов (векторы, скаляры, матрицы и т.д.) значительно расширяют возможности ИИ за счет более быстрой обработки больших массивов данных. На их основе разрабатываются современные системы идентификации лиц из открытых источников для правоохранительных органов. Новой областью применения тензоров и систем ИИ являются автоматизированные военные технологии, в частности системы, которые будет прогнозировать предположительные действия “врага” во время своих учений на основе данных о военных действиях прошлых лет и других государств.

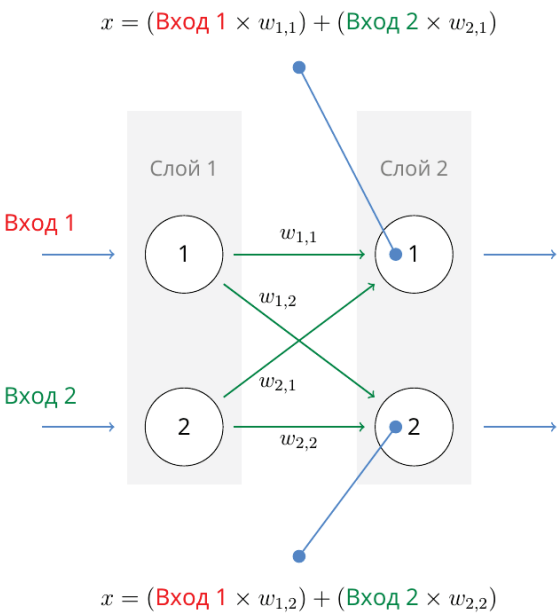


Рисунок 3 – пример использования тензоров в двухслойной нейронной сети

Список литературы:

1. Onoh G. Predicting Cyber-Attacks Using Publicly Available Data //Journal of The Colloquium for Information System Security Education (CISSE) Edition 6, Issue 1 – September 2018. [URL]. Available: https://www.researchgate.net/publication/328749220_Predicting_Cyber-Attacks_Using_Publicly_Available_Data

2. Турти М., Єрмакова А. Прогнозування захищеності інформації // Матеріали 8-ої Міжнародної науково-технічної конференції «Інформаційні системи та технології ІСТ-2019». 9-14 вересня 2019 р. Харків – Коблеве. – Харків: ХНУРЕ, 2019. – С.260-265.

3. Акивис М. А., Гольдберг В. В., Тензорное исчисление // Справочноепособие. Изд. «Наука», 1969. – 351с.

УДК 004.056.05

ПОРІВНЯЛЬНИЙ АНАЛІЗ РОЗПОВСЮДЖЕНИХ СИСТЕМ МОДЕЛЮВАННЯ МЕРЕЖ

Автор: *Тотх Мішелл, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

Науковий керівник: *Турти М.В., к.т.н., доцент, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

В даний час важко знайти область людської діяльності, в якій в тій чи іншій формі не використовувалися б методи моделювання. Формально під моделюванням розуміється заміщення одного об'єкта (оригіналу) об’єктом (моделлю), який віддзеркалює лише ті властивості реального об’єкта, що підлягають дослідженню. При моделюванні комп’ютерних мереж (КМ) практично неможливо врахувати всі впливові фактори у формальній математичній моделі. Тому при проектуванні і дослідженні КМ розповсюдженими є імітаційні моделі, які можуть бути як натурними, так і програмними. Розробка програмної імітаційної моделі КМ здійснюється за допомогою спеціального програмного забезпечення (ПЗ) – симуляторів КМ. Наявні на поточний час стимулятори різняться за виконуваними функціями і умовами застосування [1, 2].

Метою даної роботи є порівняльний аналіз сучасних засобів моделювання комп’ютерних мереж.

Для досягнення поставленої мети необхідно розв’язати наступні задачі: визначити типові завдання, які вирішуються при моделюванні захищених КМ; визначити критерії порівняння ПЗ для моделювання КМ; оцінити сучасні симулятори за цими критеріями.

Типовими завданнями, які вирішуються при імітаційному моделюванні захищених КМ є: перевірка працездатності проектованих КМ; віртуальне випробування КМ при різних навантаженнях; віртуальне випробування системи захисту КМ; оцінювання продуктивності при роботі з певними типами даних; оцінювання продуктивності по окремих сегментах і мережі в цілому; визначення і аналіз наслідків

зміни організаційної структури КМ; визначення і аналіз наслідків збоїв в роботі обладнання; визначення і аналіз наслідків впливу завад в каналах передачі даних; вибір фізичного розташування об'єктів ЛОМ; визначення розподілу завантаженості мережі та її сегментів у часі; обчислення критичного часу; оцінювання економічної ефективності обраних схемо-технічних рішень локальних обчислювальних мереж (ЛОМ) (отримана оцінка є складовою вартості проекту, при визначенні котрої мають бути враховані витрати на конфігурування мережі, навчання обслуговуючого персоналу і користувачів); оптимізація набору протоколів тощо. Вирішення цих завдань дозволяє обрати варіант виконання мережі для робочого проекту.

Як показав проведений аналіз, критерії порівняння ПЗ для моделювання КМ можуть бути представлені трьома групами критеріїв:

1. Критерії, що характеризують середовище застосування ПЗ: тип операційної системи; необхідний обсяг оперативної пам'яті; необхідний обсяг вільного дискового простору.

2. Критерії, що характеризують зручність застосування ПЗ для користувача: зручність установки; зручність налагодження; наявність довідникових, навчальних і демонстраційних матеріалів від фірми-розробника ПЗ на відповідній мові, а також на рідній мові користувача; наявність вбудованих бібліотек елементів КМ; можливість створення користувачем нових власних бібліотек елементів КМ і коригування існуючих моделей елементів КМ; дружність інтерфейсу користувача; наявність засобів візуалізації результатів роботи ПЗ у формі, необхідній користувачу; вартість; рівень довіри до фірми-розробника ПЗ; наявність підтримки ПЗ в процесі експлуатації і умови отримання нових версій.

3. Критерії, що характеризують функціональні можливості ПЗ:

а) віртуальне обладнання КМ з відповідними позначеннями і налаштуваннями: персональний комп'ютер, сервер, модем, концентратор (англ. Hub), комутатор простий (англ. Switch), комутатор багаторівневий (англ. Multilayer Switch), маршрутизатор (англ. Router), точка доступу (англ. Access Point). Моделі обладнання можуть бути двох типів:

– моделі конкретного обладнання;

– абстрактні моделі обладнання КМ, отримані в результаті узагальнення і спрощення моделей обладнання певного типу;

б) віртуальні засоби з'єднання мережевих пристроїв: кабелі з металевим середовищем передачі сигналу (консольний кабель, який підключається до портів RS-232; «прямий» мідний кабель Ehternet на основі витої пари (UTP) з розняттями RJ-45; «перехресний» мідний кабель; телефонний кабель; коаксіальний кабель); з'єднувальний кабель DCE/DTE для передачі синхросигналів; оптоволоконний кабель; радіоканал; інфрачервоний канал;

в) автоматичний вибір засобів з'єднання мережевих пристроїв в залежності від їх типу;

г) здатність працювати в режимі реального часу;

д) моделі збоїв в мережі на основі статистичних і нечітких даних;

є) моделювання генерації даних додатками;

ж) моделювання розбиття даних на датаграми, пакети та кадри протоколів, визначення затримок;

з) моделювання процесів маршрутизації;

і) моделювання процесів в локальних обчислювальних мережах (ЛОМ), в глобальних мережах (ГМ) і в сукупності ЛОМ і ГМ;

к) імпорт інформації про трафік, що отримується в реальному часі;

л) підтримка стандартних тестів вимірювання продуктивності КМ з метою отримання таких показників продуктивності як прогнозовані затримки між кінцевими і проміжними вузлами мережі; пропускні спроможності каналів; коефіцієнти використання сегментів, буферів і процесорів; позитивні і негативні викиди трафіку як функції часу і як усереднені значення;

м) визначення джерел затримок і вузьких місць мережі;

н) імітація різних режимів навантаження обладнання КМ і каналів передачі інформації та аналіз процесів, що відбуваються в реальній обчислювальній мережі (генерація даних додатками) тощо.

За переліченими вище критеріями було проведено аналіз наступних ПЗ: Prophesy, COMNET III, NetMaker XA, StressMagik, MIND, AutoNet (Designer, MeshNET, Performance – 1, Performance – 3), BONES, Opnet, Cisco Packet Tracer 6, NetEmul, GNS3. Більшість цих ПЗ є комерційними програмними продуктами, вартість яких сягає декількох десятків тисяч доларів. Вільний доступ можна отримати до останніх трьох ПЗ (Cisco Packet Tracer 6, NetEmul, GNS3).

Prophesy від American HYTech дозволяє оцінити продуктивність КМ при роботі із даними різного типу по окремих сегментах КМ і мережі в цілому та має найменшу вартість із комерційних ПЗ.

COMNET III від CACI Product виконує детальне моделювання КМ, відображаючи результати динамічно у вигляді наочної анімації результуючого трафіку. Недоліком ПЗ є висока ціна.

NetMaker XA від MakeSystems є одним з найбільш потужних ПЗ моделювання КМ із наявних на ринку. Головними недоліками NetMaker XA є висока вартість і необхідність серйозного навчання користувачів. До складу ПЗ входять розширювана бібліотека моделей мережевих пристроїв і з'єднань, модулі, що забезпечують отримання інформації про мережу та її перегляд, конфігурування КМ, моделювання та аналіз подій в КМ (зокрема, перевірку правильності аналітичних моделей, опис протоколів і перевірку протоколів, аналіз взаємодії протоколу, оптимізацію та планування КМ).

Особливістю StressMagik від NetMagicSystem є підтримка імітації різних режимів навантаження на файл-сервер (зокрема, пікового навантаження) і стандартних тестів виміру продуктивності при відносно невеликій вартості.

Opnet від MIL3 пропонує графічне середовище для моделювання та аналізу подій в КМ (Opnet дозволяє здійснити перевірку правильності аналітичних моделей, опис протоколів і перевірку протоколів, аналіз взаємодії протоколу, оптимізацію та планування КМ), моделює смугу пропускання.

MIND від Network Analysis Center – це засіб проектування і оптимізації мережі на основі даних про вартість типових конфігурацій і точного оцінювання продуктивності. Вартість найбільш повних версій MIND є найвищою серед ПЗ аналогічного призначення.

AutoNet від Network Design and Analysis Group дозволяє моделювати смугу пропускання, імітувати збої в КМ, здійснювати облік реальних даних про трафік, що надходять від мережевих аналізаторів, описувати протоколи, визначати чутливість КМ до затримок і часу відповіді, визначати вузькі місця КМ, і оцінювати економічну доцільність певних місць розташування і оновлення обладнання, варіантів зв'язку, тарифних планів і постачальників послуг. ПЗ має модульну структуру і високу сумарну вартість.

BONES від System&Networks має відносно високу вартість і забезпечує можливість дослідження впливу активності додатків, сервісів, клієнтів і серверів, і, як результат, впливу нових технологій на роботу КМ.

NetEmul – вільно розповсюджуване ПЗ, створене групою ентузіастів, яке дозволяє проектувати обчислювальні мережі, проводити їх найпростіший аналіз, наприклад відправляти пакети даних з одного комп'ютера на інший для оцінки параметрів трафіку. NetEmul містить примітивну нерозширювану бібліотеку пристроїв (персональний комп'ютер, концентратор, комутатор, маршрутизатор) та простий інтерфейс їх налаштування. Емуляція функціонування мережі – найпростіша. Емуляція програм операційних систем та віртуалізація обладнання відсутні. NetEmul непридатне для повноцінного моделювання КМ у разі реальних проектів, але часто використовується в навчальному процесі підготовки фахівців з мережевих технологій.

GNS3 – некомерційне ПЗ компанії Galaxy Technologies LLC. GNS3 містить:

– примітивну розширювану бібліотеку активних та кінцевих пристроїв;

– утиліти для програмної емуляції апаратної частини маршрутизаторів Cisco, процесорів (Intelx86, AMD64, ARM, MIPS, RISC-V, PowerPC, SPARC, SPARC64 та частково m68k), пристроїв введення-виведення, апаратної частини CiscoPIX. Повноцінна емуляція L2 комутаторів Cisco відсутня. Однак за допомогою засобів віртуалізації пристроїв бібліотеки як мережевих і кінцевих пристроїв можуть бути розширені, в результаті цей недолік повністю нівелюється;

– засоби віртуалізації пристроїв (VirtualBox, прошивки пристроїв та образів дистрибутивів операційних систем). Віртуалізація дозволяє здійснювати конфігурування пристроїв у власних середовищах без емуляції додатків/сервісів;

– утиліти, які забезпечують прямий доступ до пакетів у мережі; захоплення та фільтрацію необроблених пакетів; захоплення та аналіз трафіку, збирання статистичної інформації про нього; аналіз структури різних мережевих протоколів з можливістю «розбирання» мережевих паке-

тів з відображенням значення кожного поля протоколу будь-якого рівня), що дозволяє проводити розширений аналіз функціонування мережі.

Недоліком GNS3 є необхідність великих системних ресурсів робочої станції для повної віртуалізації пристроїв при моделюванні КМ.

Cisco Packet Tracer – це ПЗ, розроблене компанією Cisco як засіб вивчення КМ на основі обладнання Cisco. Cisco Packet Tracer є ліцензійним програмним продуктом і, в загальному випадку вільно не розповсюджується, однак в рамках міжнародної некомерційної освітньої програми Cisco Networking Academy це ПЗ розповсюджується безкоштовно. Cisco Packet Tracer 6 [2]:

– дозволяє моделювати концентратори, комутатори рівня L2 та L3 моделі OSI, маршрутизатори, міжмережні екрани Cisco ASA, кінцеві пристрої (сервери, робочі станції, ноутбуки, принтери тощо), бездротові пристрої (Wi-Fi-маршрутизатори, точки доступу), віртуальні підключення до ГМ;

– підтримує всі види зв'язків між пристроями (консольні з'єднання, кручені пари, волоконно-оптичний кабель, Serial DCE/DTE тощо);

– забезпечує конфігурування пристроїв;

– забезпечує фізичне представлення обладнання з можливістю зміни його конфігурації (додавання різних модулів, але тільки тих, що постачаються Cisco);

– забезпечує емуляцію функціонування КМ із аналізом трафіку та PDU рівнів моделі OSI та емуляцію Desktop- та системних програм операційних систем, у тому числі сервісів серверних операційних систем (DNS, DHCP, AAA тощо).

Недоліком Cisco Packet Tracer 6 є використання активних мережевих пристроїв тільки від компанії Cisco, при тому, що бібліотека пристроїв не є розширюваною. У випадку побудови КМ виключно із застосуванням мережевого обладнання Cisco з точки зору функціональних можливостей і вартості Cisco Packet Tracer є найкращим вибором.

Висновки

В ході виконання даної роботи було визначені типові завдання, які вирішуються при моделюванні захищених КМ, і критерії порівняння ПЗ для імітаційного моделювання КМ, проведене оцінювання сучасних симуляторів за цими критеріями.

Список літератури:

1. Кулаков В.Г., Леохин Ю.Л. Моделирование компьютерных сетей в симуляторе Cisco Packet Tracer 6: учеб.пособие. – М.: Изд-во МТИ, 2016. – 175 с. URL: https://cdn3.mti.edu.ru/ cloudofscience/ editions/files/2016_Kulakov_V.G._Leohin_YU.L._Modelirovanie_kompyuternyh_setej_v_simmulyatore_CISCO_PACKET_TRACER_6.pdf
2. Коровенков Д.А. Обзор программных средств моделирования и эмуляции вычислительных сетей // Материалы Университетской студенческой научно-практической конференции Калужского гос. ун-та имени К.Э. Циолковского 2021 года. – Калуга: КГУ имени К.Э. Циолковского. 2021. – С.191-198. URL: https://tksu.ru/upload/iblock/e06/cugkovxttmm16vz6v92pe8025e7rkecc/MATERIALY-USNPK.-2021.pdf.

УДК 004.056.05

ПОРІВНЯЛЬНИЙ АНАЛІЗ СУЧАСНИХ СИСТЕМ ВИЯВЛЕННЯ ВТОРГНЕНЬ

Автор: *Тотх Мішелл, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

Науковий керівник: *Турти М.В., к.т.н., доцент, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

Разом з розвитком мережевих технологій і способів ведення електронного бізнесу зростають вимоги до безпеки. Це зумовлене тим, що зловмисники і застосовувані ними технології стають все більш витонченими [1-5], а також тим, що ускладнення програмного забезпечення призводить до збільшення в ньому кількості помилок і вразливих місць. Тому система виявлення вторгнень (англ. Intrusion Detection System, IDS) – необхідна частина сучасних мережевих комплексів захисту. Створення IDS – найбільш перспективна галузь розвитку комп'ютерних технологій. Але поки ці системи недосконалі і містять в собі безліч прихованих проблем, пов’язаних з їх розгортанням, управ-

лінням, масштабуванням і підтримкою. Крім того, спостерігається велика кількість помилкових спрацьовувань систем. Часто проблема полягає в тому, що кількість виділених ресурсів на настроювання та підтримку системи виявляється недостатньою, а без правильного налаштування неможливо домогтися ефективної роботи. Досвід користувачів показує, що установка системи складає лише 15-20 відсотків від ресурсів, витрачених на забезпечення реальної безпеки. Системи виявлення вторгнень вимагають постійного адміністративного контролю. Всі зміни в конфігурації мережі і мережевого програмного забезпечення повинні постійно враховуватися в IDS. Невідповідність в конфігурації може привести до збільшення кількості помилкових спрацьовувань, а також до появи вразливостей в системі захисту інформації. Робота IDS базується на аналізі мережного трафіку і використанні методу сигнатур (шаблонів нападу). Тому для IDS гостро постає така проблема підтримки як постійне оновлення бази сигнатур. Таким чином, система виявлення вторгнень має сенс, тільки тоді, коли вона сама розвивається разом з мережею, яку вона захищає. Такий розвиток має на увазі періодичне тестування.

Метою даної роботи є отримання порівняльних оцінок сучасних систем виявлення вторгнень.

Для досягнення поставленої мети необхідно розв'язати наступні задачі:

- скласти список сучасних систем виявлення вторгнень;
- дослідити переваги кожної системи виявлення вторгнень;
- дослідити недоліки кожної системи виявлення вторгнень.
- вирішити яка система є найнадійнішою, найдієвішою і найпростішою у використанні.

Система виявлення атак (вторгнень) — програмний або апаратний засіб, призначений для виявлення фактів несанкціонованого доступу в комп'ютерну систему або мережу або несанкціонованого управління ними в основному через Інтернет. Про будь-яку активність шкідливого програмного забезпечення (ПЗ) або про порушення типової роботи централізовано збирається інформація системою управління подіями та інформацією захисту (англ.. Security Information and Event Management – SIEM).

SIEM-система обробляє дані отримані від багатьох джерел і використовує методи фільтрування тривог для розрізнення несанкціонованої активності від хибного спрацювання тривоги, про що оповіщається адміністратор або операційний центр безпеки.

Проведемо аналіз особливостей 5-ти IDS- Snort, Suricata, Bro (Zeek), OSSEC, Samhain (табл.1)

Таблиця 1 – Аналіз IDS

IDS	Характеристики за даними розробника	Примітки
Snort	– модульна структура; – потік для обробки пакетів; – наявність загальної конфігурацію і таблиці атрибутів; – проста скриптова конфігурація; – понад 200 плагінів; – плагін Framework для доступності ключових компонентів; – автоматичне виявлення портів; – автоматичне створення довідкової документації; – масштабований профіль пам'яті; – синтаксичний аналізатор правил і особливий синтаксис; – тривалий термін служби продукту; – повна підтримка; – широкий спектр адміністративних інтерфейсів; – програма ретельно перевірена, протестована і апробована.	Snort має один потік і може використовувати тільки один процесор (ядро) в кожен момент часу (одночасно).

IDS	Характеристики за даними розробника	Примітки
Suricata	– висока продуктивність за рахунок наявності багатьох потоків і масштабованої бази кодів; – універсальний движок: NIDS, NIPS, NSM, автономний аналіз; – кросплатформенність: Linux, Windows, MacOS, OpenBSD та ін.; – підтримка TCP/IP на сучасному рівні: масштабований механізм потоку, повний IPv4/IPv6, TCP-потоки і дефрагментація IP-пакетів; – парсери протоколів – декодування пакетів; – HTTP-реєстратор запитів, зіставлення ключових слів; – автонастроювання конфігурації; – вбудований апаратний прискорювач: користувач може використовувати графічні карти для перевірки мережного трафіку; – скриптовий движок, LuaJIT (Lua scripting), який може бути використаний для перевірки інформації з пакетів. Це робить складне зіставлення даних простішим за рахунок того, що користувач має можливість об'єднати кілька правил в один скрипт; – ведення журналу і аналіз прикладного рівня: захоплення і реєстрація сертифікатів TLS/SSL, HTTP і DNS-запитів; – вбудоване апаратне прискорення (GPU для сніффінгу мережі); – витягування файлів: здатність захоплювати шкідливе ПЗ, встановлене зловмисником з метою його подальшого дослідження користувачем; – постійна підтримка.	Suricata здатна запускати багато потоків одночасно, тому на думку розробників вона забезпечує використання переваг всіх доступних процесорів. Питання щодо ефективності такого підходу є дискусійним, зокрема розробники Snort вважають її недостатньою, але багатопотоковість дозволяє покращити декілька показників якості ПЗ, тому можна стверджувати, що ефективність підходу визначається відносною важливістю цих показників.

IDS	Характеристики за даними розробника	Примітки
Bro (Zeek)	– комплексне протоколювання і аналіз трафіку; – потужна і гнучка подієво-орієнтована мова скриптів (скрипти Bro); – кросплатформенність: UNIX, Linux, FreeBSD і Mac OS; – підтримка широкого спектру протоколів: DNS, FTP, HTTP, IRC, SMTP, SSH, SSL та ін.; – реалізує повністю пасивний аналіз трафіку мережевого екрану; – аналіз в реальному часі і в автономному режимі; – підтримка кластерів при великомасштабних розгортаннях; – комплексна підтримка IPv6; – наявність шаблонів IDS; – витягування файлів; – розширювана архітектура; – відмінна підтримка.	Недоліком Bro (Zeek) є складне настроювання, але це ПЗ має здатність виявляти патерни активності, які інші системи ідентифікації не можуть знайти, підтримує кластери і має розширювану архітектуру.

IDS	Характеристики за даними розробника	Примітки
OSSEC	– моніторинг цілісності файлів (англ. File Identity Monitoring, FIM); – моніторинг журналів; – виявлення rootkit; – автоматичне реагування; – архітектура клієнт-сервер; – кросплатформенність: Linux, Solaris, Windows, MacOS та ін.; – підтримка вимог щодо відповідності FIM ; – сповіщення в реальному часі і настроювані повідомлення; – інтеграція з поточною інфраструктурою; – централізований сервер для масового управління політиками; – відмінна підтримка.	OSSEC дозволяє моніторити цілісність файлів, має агентів майже для кожної операційної системи (зокрема, скомпільований агент для Windows), широкий спектр функцій і простий процес установки.
Samhain	– FIM; – моніторинг та аналіз журналу файлів; – виявлення rootkit; – моніторинг портів; – виявлення шахрайських файлів SUID і прихованих процесів; – кросплатформенність; – централізоване ведення журналу та технічне обслуговування; – архітектура клієнт-сервер (в основному) – різноманітність методів виведення (наприклад, системний журнал, електронна пошта); – здатність до використання в якості автономного додатку на одному хості; – постійна підтримка.	Недоліками Samhain є складність установки і необхідність Cygwin для Windows, а перевагами – відмінна функціональність і висока гнучкість клієнта.

Висновки

В ході виконання даної роботи було досліджено сучасні системи виявлення вторгнень, визначені їх переваги та недоліки. Як показав проведений аналіз, вирішення питання про те, яка з систем є найнадійнішою, найдієвішою і найпростішою у використанні, залежить від середовища функціонування IDS та вимог користувача, тобто повинна визначатися за окремою методикою, яка враховувала б значимість окремих показників якості ПЗ для конкретної автоматизованої системи обробки інформації.

Список літератури:

1. Бил Дж., Бейкер Э., Казуэлл Б. Snort 2.1. Обнаружение вторжений. – Бином-Пресс, 2009. – 656 с.
2. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. Учебник для вузов. – СПб.: Питер, 2010. – 944 с.
3. Статистичні данні про ризики зіткнення з веб-програмами URL: https://securelist.ru/analysis/ksb/27543/kasperskysecurity-bulletin-2015-osnovnaya-statistika-za-2015-god/.
4. Статистичні дані щодо DDoS-атак у країнах світу. URL: https://www.infowatch.ru/report2015-2016.
5. Статистичні дані, щодо витоку конфіденційної інформації. URL: https://www.antimalware.ru/.
6. Соколов М.С. Кибернетическая безопасность – понятие, значение и эволюция от военных основ к самостоятельному виду безопасности // Военное право. – 2012. – № 1. Идентификационный номер статьи в НТЦ "Информрегистр": 0421200099\001. URL: http://www.voennoepravo.ru/files/%20%D1%81%D0%BB%D1%83%D0%B6%D0%B1%D0%B0%20%D0%BF%D0%BE%20%D0%BD%D0%B0%D0%B4%D0%B7%D0%BE%D1%80%D1%83%20%D0%B2%20%D1%81%D1%84%D0%B5%D1%80%D0%B5%20%D1%81%D0%B2%D1%8F%D0%B7%D0%B8%201-2012.doc.

УДК 004.056.5: 534.843

ЗАДАЧА ОБ'ЄКТИВІЗАЦІЇ ТОНАЛЬНОГО МЕТОДУ ВИЗНАЧЕННЯ РОЗБІРЛИВОСТІ МОВИ

Автори: *Трізно С.О., студентка; Кучер В.С., студент, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

Науковий керівник: *Касьянов Ю.І., старший викладач, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

Вступ. Захист мовної інформації від витоку акустичними каналами та достовірна оцінка захищеності завжди були і будуть однією з найважливіших задач в захисті інформації на об'єктах інформаційної діяльності, що обумовлено такими її властивостями, як конфіденційність (усно робляться такі повідомлення і віддаються такі розпорядження, які не можуть бути довірені ніякому носію чи каналу зв'язку), оперативність (інформація може бути перехоплена в момент її генерації і озвучування), документальність (перехоплена мовна інформація, яка не піддавалась обробці, є юридичним документом).

Наразі в ряді провідних країн світу при нормуванні і оцінюванні захищеності мовної інформації перейшли від раніше використовуваного загальноприйнятого критерію відношення сигнал/шум в точках можливого знімання інформації до критерію розбірливості мови, який є інваріантним до виду завади і більш універсальним, що полегшує порівняння ефективності різних засобів технічного захисту та дає можливість підвищити комфорт ведення переговорів[1-3]. І хоч в Україні до сих пір використовується критерій сигнал/шум, впровадження нового критерію видається лише питанням часу. Це потребує розробки нових методів і методик.

Метою роботи є об'єктивізація тонального методу визначення розбірливості мови для адаптації його до задачі оцінювання захищеності мовної інформації.

Основна частина. Критерій розбірливості мови уже давно використовується для оцінювання якості каналів зв'язку та акустики приміщень [4-9]. Існує безліч методів визначення розбірливості мови, які розділяють на суб'єктивні та об'єктивні. До суб'єктивних методів відносяться такі, в яких мовний чи слуховий апарат людини є складовою

частиною вимірювальної системи і вони базуються безпосередньо на експертних оцінках і виконуються з участю експертів: дикторів і аудиторів. В об'єктивних методах весь вимірювальний процес виконується приладами без участі органів чуття людини.

Об'єктивні методи більш прийнятні для використання в задачах оцінювання захищеності мовної інформації, оскільки володіють більшою оперативністю і простотою вимірювання. Тому сучасні сертифіковані методики оцінювання захищеності мовної інформації базуються в основному на об'єктивному формантному методі [1-4].

Суб'єктивні методи, маючи більшу універсальність (враховують практично всі фактори, які впливають на розбірливість) і кращу точність, дуже обмежено використовуються в задачах захисту інформації через великі затрати часу та людських ресурсів. Однак їх об'єктивізація може дати достойну альтернативу формантним методам. Одним з таких методів є тональний метод.

Цей метод оснований на тому, що людина дуже точно може визначити рівень звуку, при якому він досягає порогу чутності. Рівень відчуття тону дорівнює загасанню, що вводиться в колі звуковідтворювального пристрою, до тих пір, поки не зникне чутність кожного тону. За виміряними рівнями відчуття тону за допомогою таблиць та графіків, які застосовуються при розрахунку розбірливості мови, визначають формантну розбірливість мови, а по ній – складову, словесну розбірливість і зрозумілість мови [4, 6].

Даний метод було модернізовано та адаптовано до задачі оцінки захищеності мовної інформації [10] з урахуванням наступних факторів:

– досліджується прямий акустичний (повітряний) канал витоку мовної інформації;

– рівні інформаційного сигналу в точці прийому в даному випадку будуть сумірними або нижчими рівня фонових шумів;

– необхідність максимальної оперативності, що потребує мінімізації кількості вимірювань;

– якість каналу зв'язку та захищеність інформації залежать від розбірливості мови прямо протилежно.

Схема установки для проведення експериментів приведена на рис. 1.

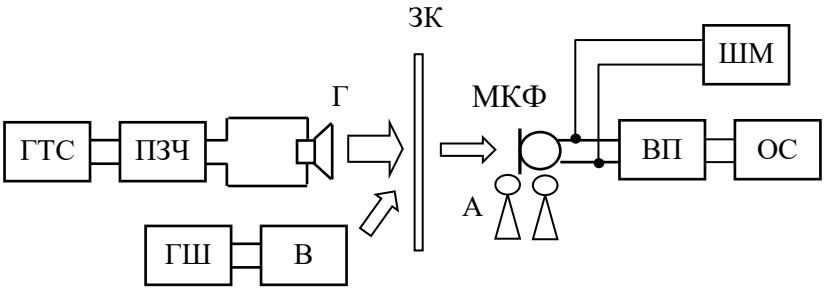


Рисунок 1 – Схема лабораторної установки: ГТС – генератор тестового сигналу; ПЗЧ –підсилювач звукової частоти; Г – гучномовець; ЗК – звукоізолююча конструкція; МКФ – вимірювальний мікрофон; А- аудитори; ВП – вимірювальний підсилювач; ШМ – шумомір; ГШ – генератор шуму; ОС – осцилограф; В – випромінювач

Вхідний тональний сигнал генерується генератором тестового сигналу ГТС або програмно на комп'ютері. Регулювання рівня звукового тиску на виході гучномовця Г може виконуватись генератором або підсилювачем ПЗЧ. Шумова завада створюється генератором шуму ГШ. Вимірювання рівнів сигналу проводиться за допомогою осцилографа ОС чи шумоміра ШМ.

Інструментальні вимірювання та подальші розрахунки виконуються для семи октавних смуг мовного діапазону з середньогеометричними частотами 125, 250, 500, 1000, 2000, 4000, 8000 Гц. Це зменшує кількість вимірювань порівняно з дослідженнями у рівноартикуляційних смугах і є типовим для оцінювання захищеності мовної інформації.

Спроба об'єктивізації була описана в [11], де вказано етапи цього процесу та наведено результати апробації. Однак, ці результати отримано в умовах, що відрізнялись від реальних, а отримані залежності погано корелюються з результатами, отриманими іншими методами в областях малих та великих відношень сигнал/шум. Ц потребує додаткових досліджень і уточнень, особливо щодо залежності порогу відчуття тону від рівня шуму в октавних смугах.

Висновок:

Для об'єктивізації тонального методу потрібно провести дослідження і узагальнення залежності порогу відчуття тону від рівня шуму в октавних смугах та провести порівняльні дослідження об'єктивізованого методу та інших методів в однакових умовах.

Список літератури:

1. Хорев А.А. (2001) Методы защиты речевой информации и оценки их эффективности. Специальная техника, № 4, С. 22 – 33.

2. Дидковский В.С., Дидковская М.В., Продеус А.Н. (2008) Акустическая экспертиза каналов речевой коммуникации. Монография. Киев, Имэкс-ЛТД, 420 с.

3. Blintsov, V., Nuzhniy, S., Parkhuts, L., Kasianov, Y. (2018). The objectified procedure and a technology for assessing the state of complex noise speech information protection. Eastern-European Journal Of Enterprise Technologies, 5 (9 (95)), 26–34. doi: http://dx.doi.org/10.15587/1729-4061.2018.144146

4. Покровский Н.Б. (1962) Расчет и измерение разборчивости речи. Москва, Гос. изд-во литературы по вопросам связи и радио, 392 с.

5. Передача речи по трактам радиотелефонной связи. Требования к разборчивости речи и методы артикуляционных измерений: ГОСТ 16600-72. – М.: ИПК Издательство стандартов, 1973. – 90 с.

6. Аппараты телефонные. Тональный метод измерения разборчивости речи: ГОСТ 8031-78. – М.: ИПК Издательство стандартов, 1998. – 6 с.

7. Передача речи по трактам связи. Методы оценки качества, разборчивости и узнаваемости : ГОСТ Р 50840-95. – М.: Госстандарт Росии, 1997.

8. *ANSI*/ASA S3.5-1997 (R2017) American National Standard Methods for Calculation of the Speech Intelligibility Index / STANDARD by American National Standards of the Acoustical Society of America, 1997.01.01

9. EN 60268-16-2011. Sound system equipment – part 16: objective rating of speech intelligibility by speech transmission index. – BSI Standards Publication, 2011. – 74 p.

10. Касьянов Ю.І., Дума С.В. (2015) Використання тонального методу визначення розбірливості мови для задачі оцінки захищеності мовної інформації. Сучасні проблеми інформаційної безпеки на транспорті: Матеріали V всеукраїнської науково-практичної конференції з міжнародною участю. Миколаїв, НУК, С. 32 – 38.

11. Касьянов Ю.І., Стаканов Д.К. (2018) Об'єктивізація тонального методу для оцінювання захищеності мовної інформації за критерієм розбірливості мови. Сучасні проблеми автоматики та електротехніки: Матеріали всеукраїнської наук.-техн. конференції. Миколаїв, НУК, С. 78 – 80.

ЗМІСТ

Наукове видання

СУЧАСНІ ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ТРАНСПОРТІ

СПІБТ–2021

IX Всеукраїнська науково-технічна конференція
з міжнародною участю

01–03 грудня 2021 року

Національний університет кораблебудування
імені адмірала Макарова
Навчально-науковий інститут автоматики та електротехніки
просп. Центральний, 3, м. Миколаїв

МАТЕРІАЛИ КОНФЕРЕНЦІЇ

(*українською, російською та англійською мовами*)

Відповідальна за випуск В. В. Трибулькевич